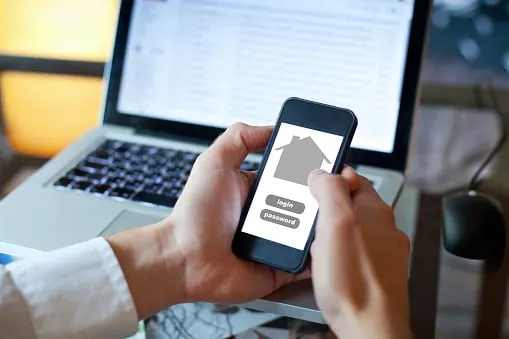
**3.-Realiza un trabajo de investigación sobre los Servidores de Acceso Remoto, que incluya la siguiente información:**

1. **Información general sobre su funcionamiento.**
2. **Protocolos de autenticación.**
3. **Ataques a los servidores remotos y sus soluciones.**

**Que es un Servidor de Acceso Remoto**

​El servidor remoto es una aplicación web que recibe y procesa las peticiones de los usuarios a través de Internet. En la mayoría de los casos, los usuarios se conectan a dichos servidores a través del servicio RRAS. Una empresa puede implantar este sistema por su cuenta o alquilar los servidores correspondientes a un proveedor de alojamiento. El concepto de "servidor remoto" fue introducido por primera vez por Microsoft. Fue esta empresa la que empezó a utilizar esta función en sus sistemas operativos Windows NT para la colaboración conjunta entre empleados.



**Funcionamiento de un Servidor de Acceso Remoto**

Los Servidores de Acceso Remoto permiten a los usuarios conectarse a una red o equipo mediante un protocolo de comunicación. Para ello, el servidor actúa como un intermediario entre el usuario y los recursos a los que se desea acceder, permitiendo la ejecución de tareas o la consulta de información como si el usuario estuviera físicamente presente.

# **Proceso Básico de Conexión**

El proceso de conexión a un servidor de acceso remoto típicamente involucra:

1. **Conexión Inicial:** El usuario se conecta al servidor a través de una red, utilizando una dirección IP o nombre de dominio.
2. **Autenticación:** El sistema solicita las credenciales del usuario (nombre de usuario y contraseña, por ejemplo) para verificar su identidad.
3. **Establecimiento de sesión:** Si las credenciales son correctas, el servidor establece una sesión que permite al usuario interactuar con los recursos de la red de manera remota

# **Tipos de Acceso Remoto**

Existen varias formas de acceso remoto, entre las más comunes se incluyen:

1. **VPN (Red Privada Virtual):** Crea un túnel seguro a través de una red pública (Internet) para permitir el acceso remoto a una red privada.
2. **Escritorio Remoto (RDP):** Permite al usuario controlar un equipo remoto de manera similar a como lo haría en el equipo local.
3. **Acceso Telnet/SSH:** Usado principalmente para administradores de sistemas, proporciona acceso a la línea de comandos de un servidor remoto

**Protocolos de autenticación de un Servidor de Acceso Remoto**

La autenticación en los servidores de acceso remoto es crucial para asegurar que solo usuarios autorizados puedan acceder a los recursos. Existen diversos métodos y protocolos de autenticación:

# **Protocolo de línea serial de Internet**

El SLIP es un protocolo antiguo para transmitir TCP/IP a través de conexiones serie, sin comprobación de errores ni cifrado. Opera en las capas física y de enlace de datos, y solo admite autenticación PAP. Su uso ha disminuido por la aparición de protocolos más avanzados.

# **Protocolo de túnel punto a punto (PPTP)**

El PPTP se usa para crear conexiones virtuales seguras entre redes a través de Internet, funcionando como una VPN. Es más barato que una conexión directa y evita costes de líneas alquiladas. Sin embargo, tiene desventajas como la configuración compleja, menor rendimiento por la tunelización, y cifrado limitado a 128 bits. Puede implementarse con dos servidores (pasarela y túnel) o con una estación de trabajo remota conectada a través de Internet.

# **Windows Remote Access Services (RAS)**

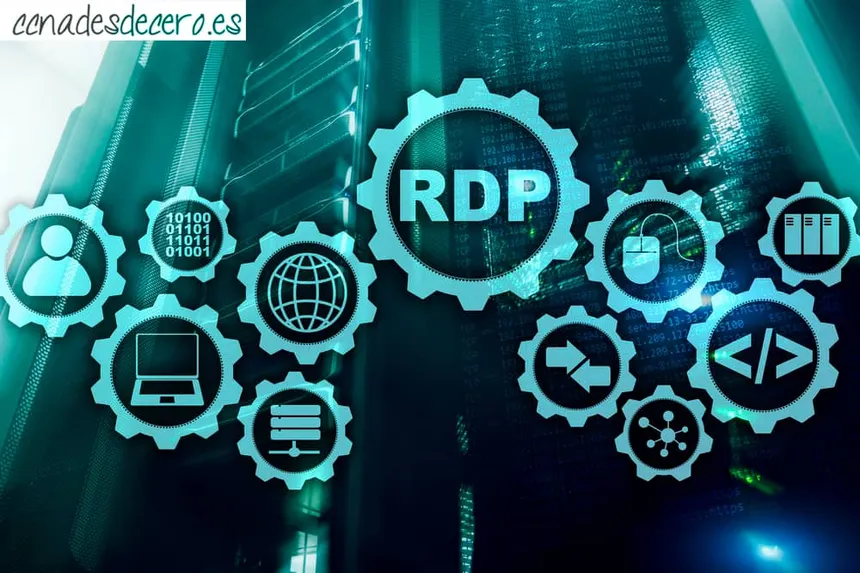
Windows NT y 2000 incluyen tecnología RAS para permitir conexiones a servidores y redes host en redes pequeñas. Con RAS, un módem puede conectarse a un servidor para realizar marcación, aunque solo permite a los usuarios acceder a la LAN, sin permitir el acceso a otros servicios como AOL.

# **Protocolo de arquitectura informática independiente (ICA)**

Los productos Citrix WinFrame (MetaFrame) y Windows Terminal Server utilizan el protocolo ICA para permitir que varios clientes livianos accedan a un ordenador virtual como si fuera su escritorio. Esto permite a las organizaciones usar estaciones de trabajo económicas como terminales, mientras actualizan solo el servidor. Sin embargo, el costo del servidor es un inconveniente. El cliente Citrix o Terminal Server se comunica con el servidor ICA, que funciona en diversas plataformas como Windows, MacOS, Linux e incluso Internet. Se requiere tener un servidor Citrix o Terminal Server para usar ICA.

# **Protocolo de escritorio remoto (RDP)**

El protocolo de escritorio remoto ofrece las mismas funciones básicas que ICA, con la salvedad de que RDP solo proporciona acceso remoto a clientes Windows.



**Ataques a un Servidor de Acceso Remoto**

Los servidores de acceso remoto son objetivos frecuentes de varios tipos de ataques, algunos de los más comunes incluyen:

# **Ataques de Fuerza Bruta**

Este tipo de ataque consiste en intentar adivinar las credenciales de acceso mediante la prueba de diferentes combinaciones de usuario y contraseña

**SOLUCIÓN:**

* Implementar políticas de contraseñas fuertes (longitud mínima, caracteres especiales, etc.).
* Limitar los intentos de inicio de sesión fallidos y bloquear la cuenta después de varios intentos fallidos.
* Utilizar autenticación multifactor (2FA) para hacer más difícil la tarea del atacante.

# **Phishing**

Consiste en el envío de correos electrónicos o enlaces fraudulentos que intentan engañar a los usuarios para que ingresen sus credenciales en sitios web falsificados

**SOLUCIÓN:**

* Capacitar a los usuarios sobre los peligros del phishing y cómo reconocer correos electrónicos sospechosos.
* Implementar filtros de correo electrónico avanzados para detectar y bloquear correos de phishing.

# **Ataques Man-in-the-Middle**

Durante la transmisión de datos entre el usuario y el servidor, un atacante intercepta y manipula la información, como las credenciales de inicio de sesión

**SOLUCIÓN:**

* Utilizar protocolos de comunicación seguros como SSL/TLS para cifrar el tráfico entre el cliente y el servidor.
* Implementar autenticación mutua, donde tanto el servidor como el cliente se autentican entre sí.

# **Ataques de Denegación de Servicio (DDoS)**

Consisten en abrumar al servidor con un gran volumen de tráfico para que se vuelva inaccesible

**SOLUCIÓN:**

* Implementar firewalls de aplicaciones web (WAF) que puedan detectar y bloquear tráfico malicioso.
* Utilizar redes de distribución de contenido (CDN) y servicios de mitigación de DDoS.