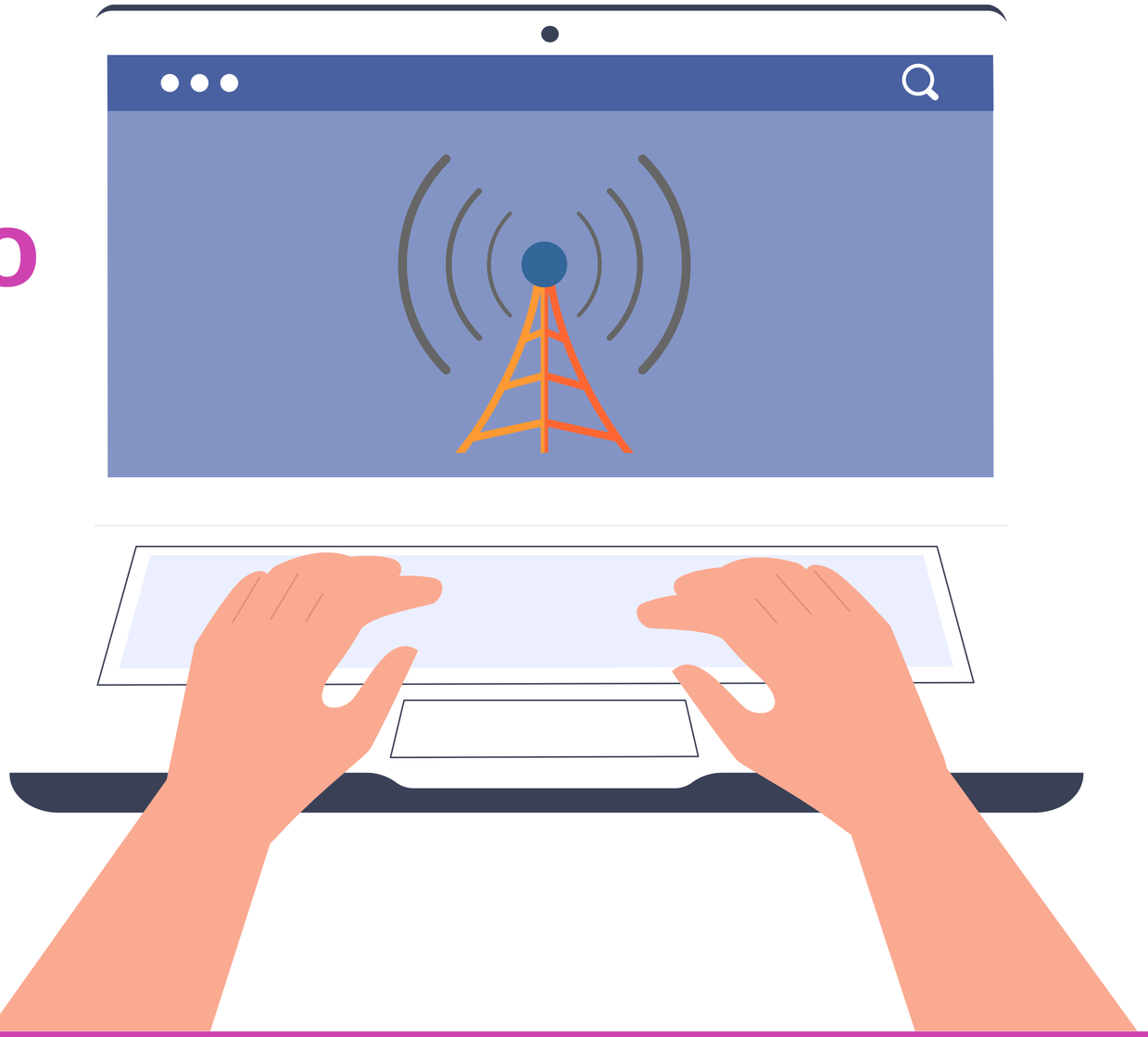
Ministerio de Educación
Gobierno de Chile

UNIVERSIDAD CATÓLICA DE TEMUCO

Protocolos de acceso remoto



Módulo 5: **Configuración de la seguridad en redes de área local.**

Conectividad y Redes

Objetivos de Aprendizaje de la Especialidad

Módulo 1	**OA1** Leer y utilizar técnicamente proyectos de conectividad y redes, considerando planos o diagramas de una red de área local (red LAN), basándose en los modelos TCP/IP y OSI. **OA3** Instalar y mantener cableados estructurados, incluyendo fibra óptica, utilizados en la construcción de redes, basándose en las especificaciones técnicas correspondientes. **OA7** Instalar y configurar una red inalámbrica según tecnologías y protocolos establecidos.
Módulo 2	**OA2** Instalar y configurar sistemas operativos en computadores personales con el fin de incorporarlos a una red LAN, cumpliendo con los estándares de calidad y seguridad establecidos. **OA11** Armar y configurar un equipo personal, basándose en manuales de instalación, utilizando las herramientas apropiadas y respetando las normas de seguridad establecidos.
Módulo 3	**OA8** Aplicar herramientas de software que permitan obtener servicios de intranet e internet de manera eficiente.
Módulo 4	**OA4** Realizar pruebas de conexión y señales en equipos y redes, optimizando el rendimiento de la red y utilizando instrumentos de medición y certificación de calidad de la señal, considerando las especificaciones técnicas.
Módulo 5	OA5 Aplicar métodos de seguridad informática para mitigar amenazas en una red LAN, aplicando técnicas como filtrado de tráfico, listas de control de acceso u otras.
Módulo 6	**OA9** Mantener y actualizar el hardware de los computadores personales y de comunicación, basándose en un cronograma de trabajo, de adcuerdo a las especificaciones técnicas del equipo.
Módulo 7	**OA10** Mantener actualizado el software de productividad y programas utilitarios en un equipo personal, de acuerdo a los requerimientos de los usuarios.
Módulo 8	**OA6** Aplicar procedimientos de recuperación de fallas y realizar copias de respaldo de los servidores, manteniendo la integridad de la información.
Módulo 9	No esta asociado a Objetivos de Aprendizaje de la Especialidad (OAE), sino a Genéricos. No obstante, puede asociarse a un OAE como estrategia didáctica.

Perfil de Egreso – Objetivos de Aprendizaje Genéricos

A- Comunicarse oralmente y por escrito con claridad, utilizando registros de habla y de escritura pertinentes a la situación laboral y a la relación con los interlocutores.	**B-** Leer y utilizar distintos tipos de textos relacionados con el trabajo, tales como especificaciones técnicas, normativas diversas, legislación laboral, así como noticias y artículos que enriquezcan su experiencia laboral.	**C-** Realizar las tareas de manera prolija, cumpliendo plazos establecidos y estándares de calidad, y buscando alternativas y soluciones cuando se presentan problemas pertinentes a las funciones desempeñadas.
D- Trabajar eficazmente en equipo, coordinando acciones con otros in situ o a distancia, solicitando y prestando cooperación para el buen cumplimiento de sus tareas habituales o emergentes.	**E-** Tratar con respeto a subordinados, superiores, colegas, clientes, personas con discapacidades, sin hacer distinciones de género, de clase social, de etnias u otras.	**F-** Respetar y solicitar respeto de deberes y derechos laborales establecidos, así como de aquellas normas culturales internas de la organización que influyen positivamente en el sentido de pertenencia y en la motivación laboral.
G- Participar en diversas situaciones de aprendizaje, formales e informales, y calificarse para desarrollar mejor su trabajo actual o bien para asumir nuevas tareas o puestos de trabajo, en una perspectiva de formación permanente.	**H-** Manejar tecnologías de la información y comunicación para obtener y procesar información pertinente al trabajo, así como para comunicar resultados, instrucciones e ideas.	**I-** Utilizar eficientemente los insumos para los procesos productivos y disponer cuidadosamente los desechos, en una perspectiva de eficiencia energética y cuidado ambiental.
J- Emprender iniciativas útiles en los lugares de trabajo y/o proyectos propios, aplicando principios básicos de gestión financiera y administración para generarles viabilidad.	**K-** Prevenir situaciones de riesgo y enfermedades ocupasionales, evaluando las condiciones del entorno del trabajo y utilizando los elementos de protección personal según la normativa correspondiente.	**L-** Tomar decisiones financieras bien informadas, con proyección a mediano y largo plazo, respecto del ahorro, especialmente del ahorro previsional, de los seguros, y de los riesgos y oportunidades del endeudamiento crediticio así como de la inversión.

Marco de Cualificaciones Técnico Profesional (MCTP) Nivel 3 y su relación con los OAG

HABILIDADES

1. Información
1. Analiza y utiliza información de acuerdo a parámetros establecidos para responder a las necesidades propias de sus actividades y funciones.
2. Identifica y analiza información para fundamentar y responder a las necesidades propias de sus actividades.

2. Resolución de problemas
1. Reconoce y previene problemas de acuerdo a parámetros establecidos en contextos conocidos propios de su actividad o funcion.
2. Detecta las causas que originan problemas en contextos conocidos de acuerdo a parámetros establecidos.
3. Aplica soluciones a problemas de acuerdo a parámetros establecidos en contextos conocidos propios de una función.

3. Uso de recursos
1. Selecciona y utiliza materiales, herramientas y equipamiento para responder a una necesidad propia de una actividad o función especializada en contextos conocidos.
2. Organiza y comprueba la disponibilidad de los materiales, herramientas y equipamiento.
3. Identifica y aplica procedimientos y técnicas específicas de una función de acuedo a parámetros establecidos.

4. Comunicación
4. Comunica y recibe información relacionada a su actividad o función, a través de medios y soportes adecuados en contextos conocidos.

APLICACIÓN EN CONTEXTO

5. Trabajo con otros
1. Trabaja colaborativamente en actividades y funciones coordinándose con otros en diversos contextos.

6. Autonomía
1. Se desempeña con autonomía en actividades y funciones especializadas en diversos contextos con supervisión directa.
2. Toma decisiones en actividades propias y en aquellas que inciden en el quehacer de otros en contextos conocidos.
3. Evalua el proceso y el resultado de sus actividades y funciones de acuerdo a parámetros establecidos para mejorar sus prácticas.
4. Busca oportunidades y redes para el desarrollo de sus capacidades

7. Ética y responsabilidad
1. Actúa de acuerdo a las normas y protocolos que guían su desempeño y reconoce el impacto que la calidad de su trabajo tiene sobre el proceso productivo o la entrega de servicios.
2. Responde por cumplimiento de los procedimientos y resultados de sus actividades.
3. Comprende y valora los efectos de sus acciones sobre la salud y la vida, la organización, la sociedad y el medio ambiente.
4. Actúa acorde al marco de sus conocimientos. experiencias y alcance de sus actividades y funciones

CONOCIMIENTO

8. Conocimientos
1. Demuestra conocimientos especificos de su área y de las tendencias de desarrollo para el desempeño de sus actividades y funciones.

Metodología seleccionada

Demostración guiada

- Esta presentación te servirá para avanzar paso a paso en el desarrollo de la actividad propuesta.

Aprendizaje Esperado

- **5.3** Configura el acceso a una red de área local utilizando protocolos para la administración remota de la red respetando la normativa legal vigente.

¿Qué vamos a lograr con esta actividad para llegar al Aprendizaje Esperado (AE)?

Reconocer las características y seguridad asociadas para el protocolo TELNET y SSH, además de crear usuarios y permisos para el ingreso a ambos protocolos.

Contenidos

01 Entender las características de los protocolos de acceso remoto.

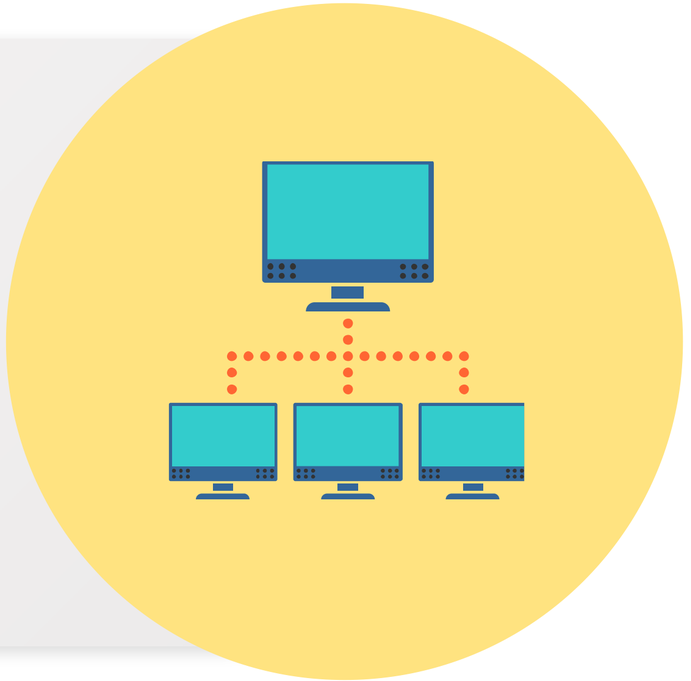
02 Entender la seguridad asociada a los protocolos de acceso remoto.

03 Configurar protocolo de acceso remoto TELNET.

04 Configurar protocolo de acceso remoto SSH.

05 Crear cuentas con permisos de usuario para el acceso a TELNET o SSH.

¿Cómo puedo acceder de forma remota a un dispositivo?



TELNET

01

- **TELNET** es un protocolo de acceso remoto, trabaja con el protocolo de transporte **TCP** y responde al puerto 23.

02

- En cuanto a la seguridad, **TELNET** es un protocolo que su tráfico se envía en texto plano, esto quiere decir, que el usuario , contraseña y configuraciones se pueden ver con un analizador de tráfico igual como fueron digitadas.

Ejemplo

- Si mi usuario es Juan y la contraseña es 1234, con el analizador de tráfico se verá exactamente igual.

SSH

01

- SSH es un protocolo de acceso remoto , trabaja con el protocolo de transporte TCP y responde al puerto 22.

02

- En cuanto a la seguridad, SSH es más seguro que TELNET, ya que su tráfico se envía cifrado. Esto quiere decir que usuario, contraseña y configuraciones se ven de forma ilegible en un analizador de tráfico.

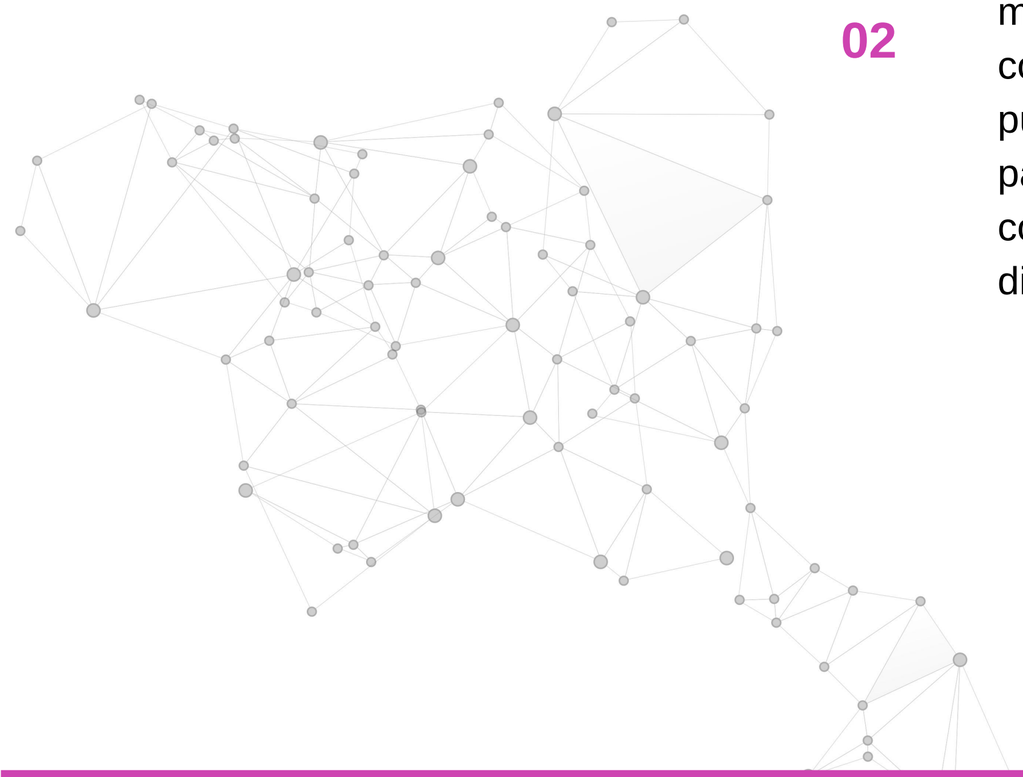
Ejemplo

- Si mi usuario es Juan y la contraseña es 1234 con el analizador de tráfico se verá usuario !”#$%&/ contraseña)=(/&%$#”. Este código es solo un ejemplo para que se entienda el concepto.

Crear usuarios y permisos

01

- La creación de usuarios con su



02

- Generalmente, se crean usuarios que tienen la capacidad de poder modificar o crear nuevas configuraciones, o usuarios que sólo pueden revisar las configuraciones para redactar informes sobre las configuraciones que existen en dicho dispositivo.

Ejemplo

- Los permisos para Cisco se configuran como privilegios que van de 0 a 15, siendo el privilegio 15 permiso de administrador, como se puede apreciar en la configuración. Para otras marcas tienen una lógica similar tanto para crear usuario, como para establecer contraseña y asignar permisos.

Diagrama TELNET

- TELNET ACCESO REMOTO

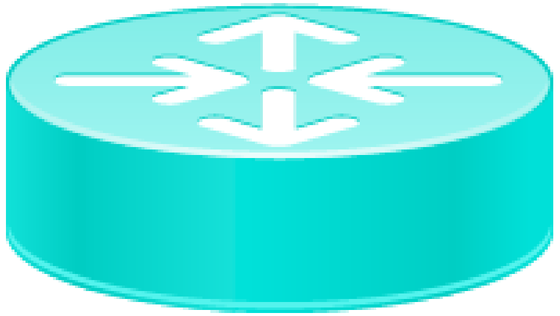


Imagen: fuente propia

Pregunta de reflexión

¿Cuál es la importancia de la configuración de usuarios y permisos?

Configuración TELNET-SSH

- Los siguientes **ejemplos** de configuración están sobre simulador **CISCO Packet Tracer**, y éstas configuraciones son aplicables en equipamiento real **CISCO**.

Configuración TELNET

Los pasos a seguir para su configuración son:

1. Conexión de equipos (cableado).
2. Configurar direccionamiento IP.
3. Configurar comandos del protocolo TELNET.
4. Configuración usuario con permisos de administrador para el ingreso a TELNET.

Configuración TELNET

- Se establecen las líneas virtuales, en este caso 0 a 4. Esto quiere decir que se pueden conectar 5 usuarios a acceso remoto. Luego se establece que para ingresar se necesita un usuario y contraseña (login local) y que sólo aceptará el ingreso a **TELNET.**

```
line vty 0 4
 login local
 transport input telnet
```

Imagen: fuente propia

Verificación Ingreso TELNET

- En la imagen se puede apreciar que me conecto a la IP del dispositivo de red desde un PC para el acceso remoto.

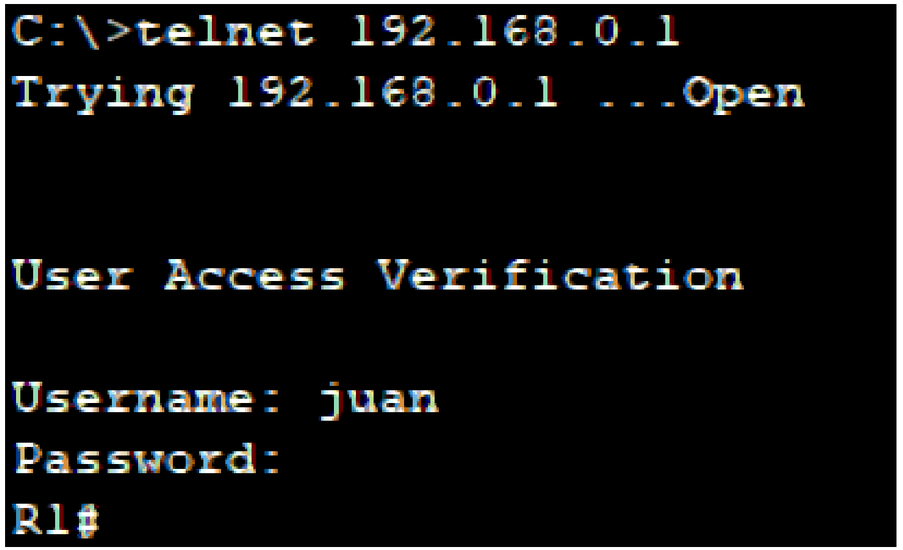


Imagen: fuente propia

Diagrama TELNET

- SSH ACCESO REMOTO

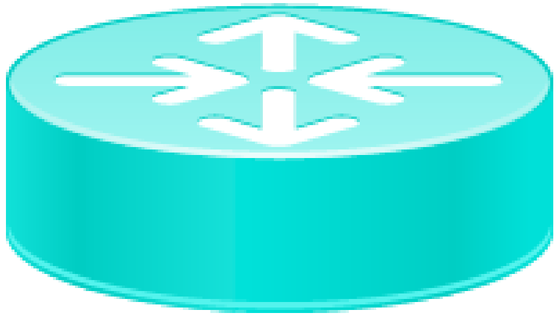


Imagen: fuente propia

Pregunta de reflexión

Para esta configuración: ¿En qué casos es más adecuado usar TELNET?

Configuración SSH

Los pasos a seguir para su configuración son:

1. Conexión de equipos (cableado).
2. Configurar direccionamiento IP.
3. Configurar comandos del protocolo SSH.
4. Configuración usuario con permisos de administrador para el ingreso a SSH.

Configuración SSH

- Se establecen las líneas virtuales, en este caso 0 a 4, esto quiere decir se pueden conectar 5 usuarios a acceso remoto , luego se establece que para ingresar se necesita un usuario y contraseña (login local) y que sólo aceptará el ingreso a **SSH.**

```
line vty 0 4
 login local
 transport input ssh
```

Imagen: fuente propia

Configuración SSH

- Se establecen la versión de SSH a utilizar y un dominio.

```
line vty 0 4
 login local
 transport input ssh
```

Imagen: fuente propia

Configuración SSH

- Se debe generar claves secretas para que el dispositivo de red encripte el tráfico SSH. La clave es precisamente lo que se utiliza para cifrar y descifrar datos. Para crear una clave de encriptación, utilice el comando **crypto key generate rsa** *tamaño-del-módulo.*

```
R1(config)#crypto key generate rsa
The name for the keys will be: R1.ejemplo.cl
Choose the size of the key modulus in the range of 360 to 2048 for
your
  General Purpose Keys. Choosing a key modulus greater than 512 may
take
  a few minutes.

How many bits in the modulus [512]: 1024
```

Imagen: fuente propia

Verificación Ingreso SSH

- En la **imagen** se puede apreciar que me conecto a la IP del dispositivo de red desde un PC para el acceso remoto.

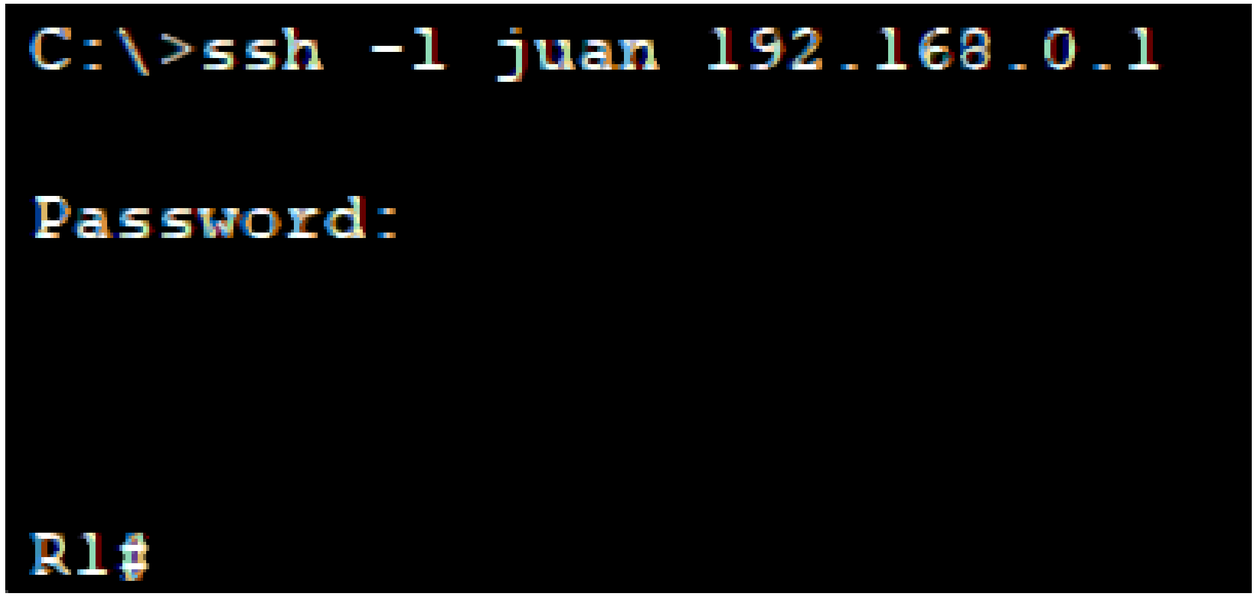


Imagen: fuente propia

Amenazas y aspectos Legales

- Si bien es cierto, el acceso remoto a computadores facilita las tareas de mantenimiento y soporte a los usuarios, entre otros beneficios, también es cierto que puede constituir un peligro al propiciar el acceso a sistemas ajenos, ejecutar código, infectarlos, obtener información confidencial de la organización, como si fuera un usuario legítimo.

- Este tipo de acciones **constituyen un delito tipificado y penalizado en las leyes chilenas.**

- **La Ley N° 19.628** regula el trato de los datos de carácter personal, en registros o bancos de datos, por organismos públicos o privados, y es uno de los estatutos normativos más relevantes sobre la materia.

- **La Ley 19223** Tipifica Figuras Penales Relativas a la Informática.

- **Artículo 2°.-** El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Pregunta de reflexión

¿Cuáles son las fortalezas de SSH por sobre TELNET ?

Ticket de salida

01

Individualmente, indica 2 eventos que lograste monitorear.

02

Discute con un compañero o compañera ¿Qué paso se te dificultó al implementar un monitoreo del sistema?¿Por qué? ¿Cómo lo resolviste?

03

Si te preguntaran sobre la razón de monitorear un sistema, ¿qué razones darías?

04

Del trabajo en equipo, ¿que mejorarían en el futuro para hacer una tarea de mejor calidad?

Referencias

Currículo CISCO CCNA 200-301.

Biblioteca del Congreso Nacional de Chile, Ley 19223 Tipifica Figuras Penales Relativas a la Informática.

Biblioteca del Congreso Nacional de Chile, Ley 19628, LEY 19628 Sobre Protección de la Vida Privada.

¿Preguntas?