Redes y comunicación de Datos 2

Sesión 11

Ciclo: Agosto 2024

Universidad Tecnológica del Perú

Temario

- Presentación del logro de la sesión.
- Dinámica: Lluvia de ideas sobre la seguridad de la LAN.
- Conceptos de seguridad de la LAN
- Evolución de las Tecnologías de la Información.
- Seguridad de la Información.
- Riesgos para los Sistemas de la Información.
- Hackers
- Clases de Ataques
- Mecanismos de defensa.
- **Actividad:**
  - ***Explicar la seguridad de la LAN.***

Logro general

Al finalizar el curso, el estudiante implementa soluciones para problemas de redes y comunicaciones de área local y extendida, empleando tecnología de interconexión y seguridad, según las necesidades planteadas.

Logro de aprendizaje de la sesión

Al finalizar la unidad, el estudiante explica cómo las vulnerabilidades ponen riesgo la seguridad LAN, para mitigar algunos ataques informáticos, a través de ejemplos desarrollados en clase.

Buenas Prácticas

Buenas Prácticas

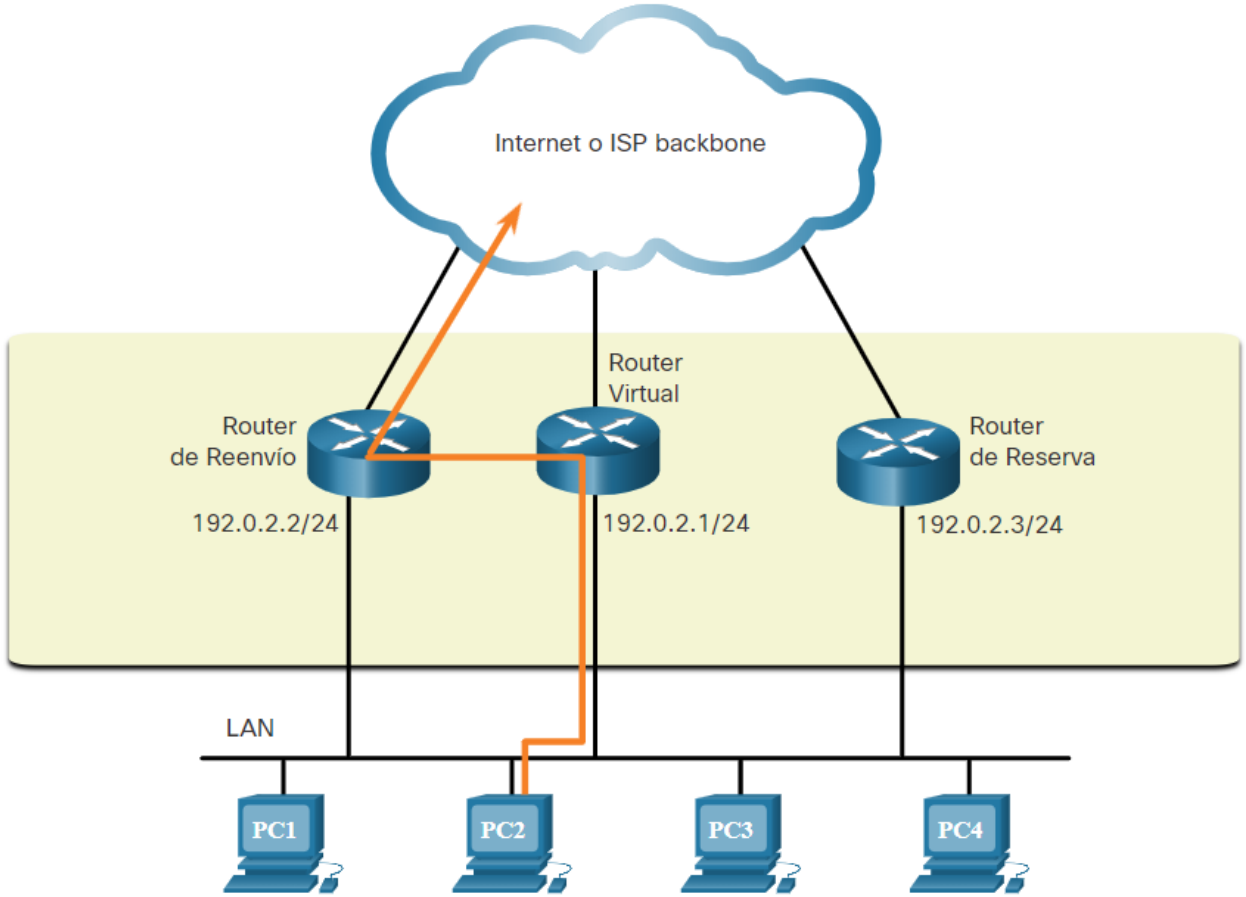
Con respecto a la Sesión 9

- ¿Qué temas desarrollamos?
- Podrias comentarme de manera breve por favor.

Recuerda que es importante que revises el material de clases de cada semana.

Redundancia del Router

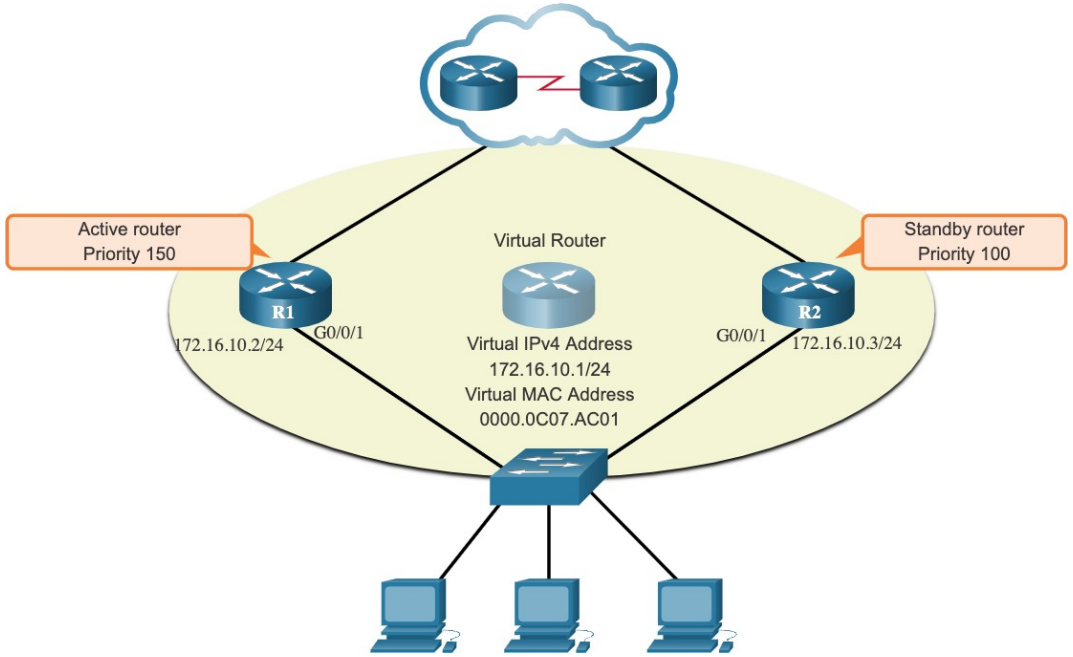
Una forma de evitar un único punto de falla en el gateway predeterminado es implementar un router virtual. Como se muestra en la figura, para implementar este tipo de redundancia de router, se configuran varios routers para que funcionen juntos y así dar la sensación de que hay un único router a los hosts en la LAN. Al compartir una dirección IP y una dirección MAC, dos o más routers pueden funcionar como un único router virtual.



Prioridad e Intento de Prioridad del HSRP

El rol de los routers activos y de reserva se determina durante el proceso de elección del HSRP. De manera predeterminada, el router con la dirección IPv4 numéricamente más alta se elige como router activo. Sin embargo, siempre es mejor controlar cómo funcionará su red en condiciones normales en lugar de dejarlo librado al azar.

- La prioridad HSRP se puede utilizar para determinar el router activo.
- El router con la prioridad HSRP más alta será el router activo.
- De manera predeterminada, la prioridad HSRP es 100.
- Si las prioridades son iguales, el router con la dirección IPv4 numéricamente más alta es elegido como router activo.
- Para configurar un router para que sea el router activo, utilice el comando de interfaz **standby priority** . El rango de prioridad HSRP es de 0 a 255.



Buenas Prácticas

Sesión 9

Lluvia de ideas sobre la capa enlace de datos

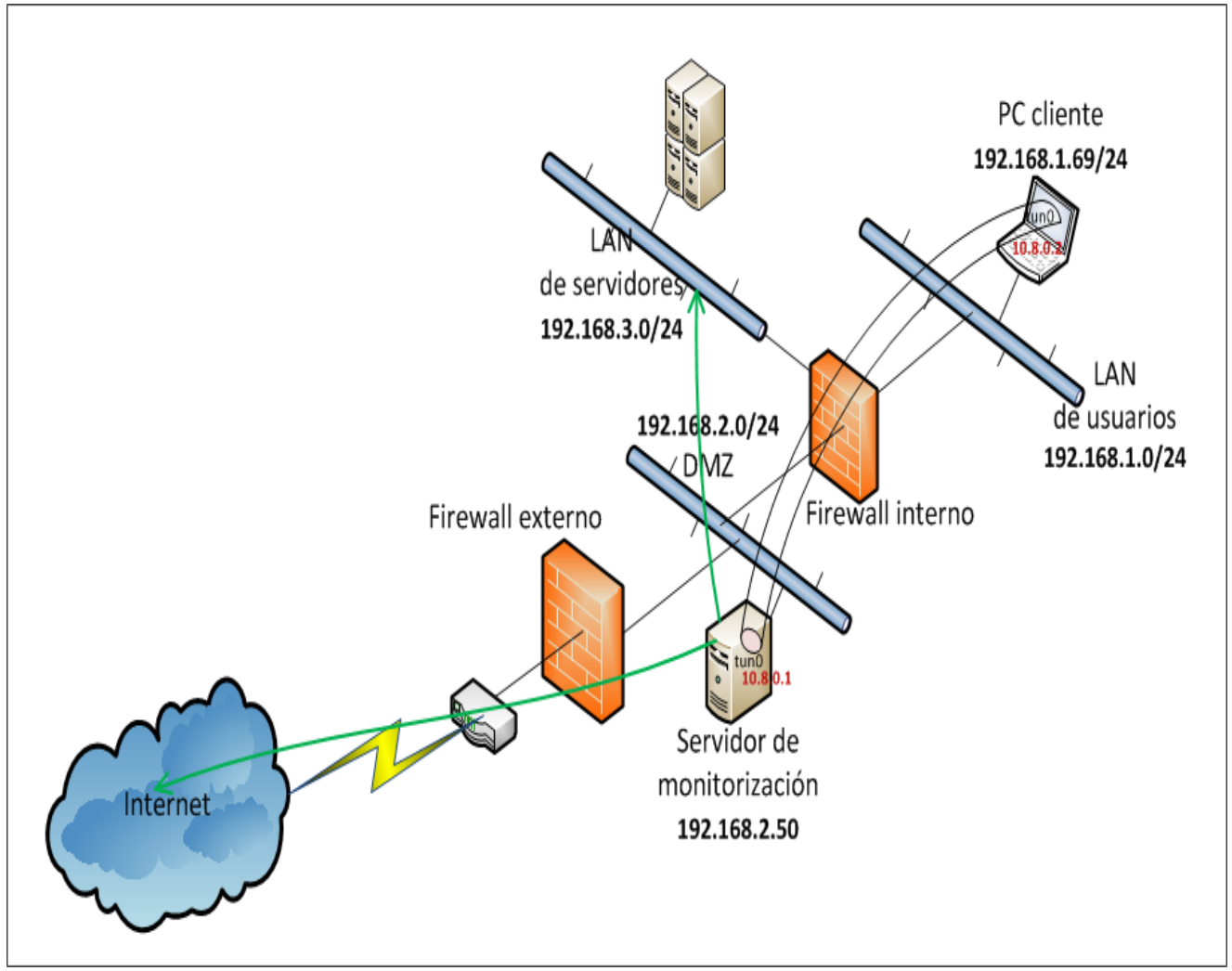
- ¿Qué es la seguridad LAN?
- ¿Para qué sirve la seguridad LAN?

Seguridad LAN

Conceptos de seguridad de la LAN

La seguridad de red es cualquier actividad diseñada para proteger el acceso, el uso y la integridad de la red y los datos corporativos.

- Incluye tecnologías de hardware y software.
  - Está orientada a diversas amenazas.
    - Evita que ingresen o se propaguen por la red.
  - La seguridad de red eficaz administra el acceso a la red.



Evolución de las Tecnologías de la Información

- La **información** es uno de los principales activos de una empresa.
- Las empresas almacenan y gestionan la información en los **Sistemas de Información**.
- En todas las empresas es fundamental proteger sus sistemas de Información, con el objetivo de mantener a salvo su información.

Evolución de las Tecnologías de la Información

Dificultades:

- El entorno donde las empresas desarrollan sus actividades es cada vez más complejo debido al desarrollo de las tecnologías de información y otros factores del entorno empresarial

- El perfil de un ciberdelincuente de un sistema informático ha cambiado radicalmente. Si bien antes los objetivos podían ser más simple (acceder a un sitio donde nadie antes había conseguido llegar). En la actualidad los atacantes se han percatado de lo importante que es la información y sobre todo de lo valiosa que puede llegar a ser.

Evolución de las Tecnologías de la Información

Es fundamental poner los medios técnicos y organizativos necesarios para garantizar la seguridad de la información. Para lograrlo hay que garantizar la **confidencialidad, integridad, disponibilidad** de la información.

Casos Notorios

Universidad Tecnológica del Perú

Seguridad de la Información

La seguridad de la información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información:

- **Confidencialidad**
  - **Integridad**
    - **Disponibilidad**
      - **Autenticidad**
        - **No repudio**

Riesgo para los Sistemas de la Información

¿Qué son los riesgos en los sistemas de información?

Las amenazas sobre la información almacenada en un sistema informático.

Ejemplos de riesgos en los sistemas de información:

- **Daño físico**
- **Acciones humanas**
- **Fallos del equipamiento**
- **Ataques internos o externos**
- **Pérdida de datos**
- **Errores en las aplicaciones**

Hacker

La figura del Hacker

¿Qué es un hacker?

La figura del Hacker

¿Qué tipos de hackers existen en función de los objetivos que tienen?

Black Hat Hackers

White Hat Hackers

Gray (Grey) Hat Hackers

Clases de Ataques

- **Interrupción:** se produce cuando un recurso, herramienta o la propia red deja de estar disponible debido al ataque.
- **Intercepción:** se logra cuando un tercero accede a la información del ordenador o a la que se encuentra en tránsito por la red.
- **Modificación:** se trata de modificar la información sin autorización alguna.
- **Fabricación**: se crean productos, tales como páginas web o tarjetas magnéticas falsas.

Técnicas de hacking

- ✓ Spoofing
- ✓ Sniffing
- ✓ Man in the middle
- ✓ Malware
- ✓ Denegación de servicio
- ✓ Ingeniería social

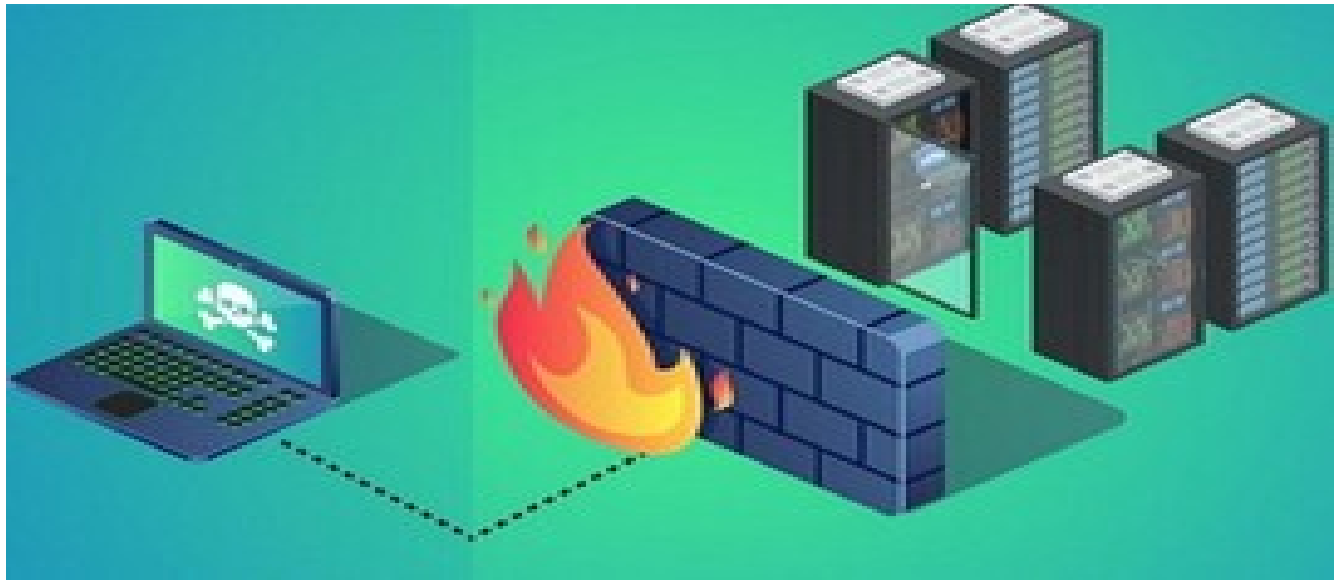
Mecanismos de defensa

Mecanismos de defensa

¿cómo pueden protegerse las compañías con las nueva tecnologías?

Los principales sistemas y más conocidos son los siguientes:

- **Firewall:** es un sistema de seguridad de red de las computadoras que restringe el tráfico de Internet entrante, saliente o dentro de una red privada. Es decir son sistemas de restricción de tráfico basado en reglas.



Mecanismos de defensa

- **Sistemas IDS/IPS:** sistemas de monitorización, detección y/o prevención de accesos no permitidos en una red.

Mecanismos de defensa

- **Honeypot:** equipos aparentemente vulnerables diseñados para atraer y detectar a los atacantes, protegiendo los sistemas realmente críticos.

- **SIEM:** La Administración de eventos e información de seguridad, es una solución de seguridad que ayuda a las organizaciones a detectar y analizar amenazas y responder a ellas antes de que afecten las operaciones del negocio.

- **Antimalware:** sistemas de detección de malware informático.

¿Qué es la explotación de sistemas informáticos?

- **Página web**: programas orientados a internet soportados por servidores web.
  - El código fuente es interpretado por el servidor.
  - El servidor gestiona las conexiones y actúa como intermediario.
  - El servidor está soportado por una infraestructura similar a un ordenador.

- **Explotación de aplicaciones web:** aprovechamiento de fallos de seguridad en el código fuente.
  - Sistemas de autenticación y autorización.
  - Inyección de caracteres.
  - Intrusión a través de fallos de programación.

¿Qué es la explotación de sistemas informáticos?

Explotación de sistemas: aprovechamiento del servidor y de la infraestructura.

- Uso de puntos de entrada.
- Identificación de protocolos débiles.
- Explotación de fallos de seguridad de software

Donde existen más riesgos para dichos ataques

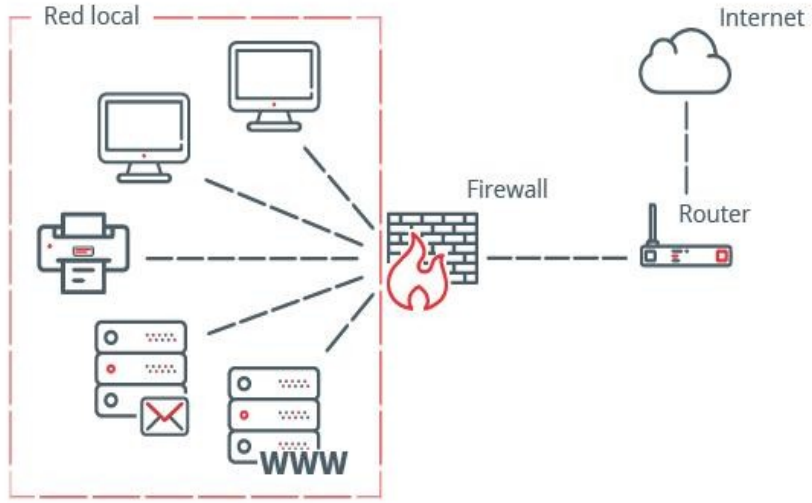
Riesgo en LANs >> Riesgo en Internet.

- **LANs (Redes de Área Local):**
  - Conectividad muy alta.
  - Capacidad de escucha de la red.
  - Pocos dispositivos intermedios.
  - Normalmente sin dispositivos de seguridad.
  - Difíciles de configurar.
  - Ataques menos ruidosos.

- **Internet**:
  - Menor capacidad de conexión.
  - Muchos dispositivos intermedios.
  - Muchos dispositivos de seguridad.
  - Mucha mayor exposición a posibles atacantes.
  - Ataque rastreable si no se toman precauciones.

¿Qué riesgos corremos como usuarios?

- Blanco directos en redes de área local y en redes WiFi:
  - Bibliotecas.
  - Cafeterías.
  - Aeropuertos.
  - Etc.



- De manera indirecta en internet:
  - Existen organizaciones dedicadas a buscar servidores vulnerables.
  - Una vez explotan dichos servidores, alojan malware en los mismos.
  - De manera que los usuarios sean infectados tras visitarlos.

¿Qué son los puertos?

- Interfaz para comunicarse con un programa especifico a través de la red.
- Cada puerto únicamente puede proveer un servicio de forma simultánea.
- Estado de los puertos:
  - Abierto: en dicho puerto se provee un servicio.
  - Filtrado: un firewall está restringiendo la conexión.
  - Cerrado: en dicho puerto no se provee un servicio.
- Algunos puertos y sus servicios más comunes:

Puerto	Servicio
21	FTP
22	SSH
23	TELNET
53	DNS
80	HTTP
443	HTTPS

¿Qué son los servicios

- Son los programas que se están ejecutando en cada uno de los puertos.
- Algunos servicios comunes y su función:
  - **FTP:**
    - Protocolo para la transferencia de ficheros.
    - Por defecto en el puerto 21.
  - **TELNET:**
    - Protocolo para el control remoto de sistemas a través de comandos.
    - Por defecto en el puerto 23.
  - **DNS:**
    - Protocolo para la resolución de nombres de dominio.
    - Por defecto en el puerto 53.
  - **HTTP:**
    - Protocolo utilizado para la comunicación con aplicaciones web.
    - Por defecto en el puerto 80.
  - **HTTPS:**
    - Protocolo utilizado para la comunicación cifrada con aplicaciones web.
    - Por defecto en el puerto 443.

¿Preguntas?

Actividades

Laboratorio especializado

Los estudiantes resuelven la siguiente actividad.

Actividades

- ¿Qué son los riesgos en los sistemas de información?
- ¿Qué otra amenaza se te ocurre?
- ¿Qué es un hacker?
- ¿Qué tipos de hackers existen en función de los objetivos que tienen?
- ¿Qué métodos emplea para protegerse contra el SPAM y el phishing?
- ¿Cómo pueden protegerse las compañías con las nuevas tecnologías?
- ¿Por qué es tan importante la seguridad de capa 2?

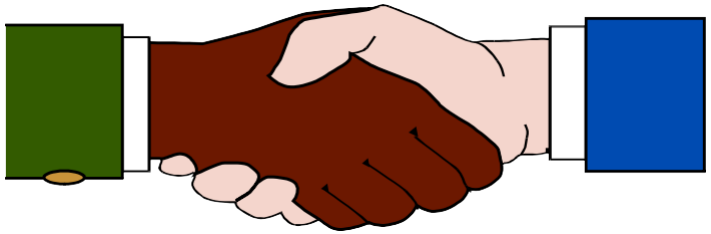
Conclusiones

¿Qué aprendí en esta sesión?

¿Qué aprendí en está sesión?

- La seguridad de la red es ahora una parte integral de las redes informáticas.
- La seguridad de la red incluye protocolos, tecnologías, dispositivos, herramientas y técnicas para proteger los datos y mitigar las amenazas.
- La seguridad de la red está impulsada en gran medida por el esfuerzo de ir un paso por delante de los piratas informáticos mal intencionados.
- Se han creado organizaciones de seguridad de redes para establecer comunidades formales de profesionales de seguridad de redes.
- La complejidad de la seguridad de la red hace que sea difícil dominar todo lo que abarca.
- Diferentes organizaciones han creado dominios que subdividen el mundo de la seguridad de redes en partes más manejables.
- Esta división permite a los profesionales centrarse en áreas de especialización más precisas en su formación, investigación y empleo.

Gracias



Universidad
Tecnológica
del Perú