UNIVERSIDAD DEL SURESTE

SAN CRISTOBAL DE LAS CASAS CHIAPAS

MATERIA: BASE DE DATOS I

TRABAJO: MAPA CONCEPTUAL

NOMBRE DEL ALUMNO: BALDOMERO SANTIZ GOMEZ

SEMESTRE: 7MO. CUATRIMESTRE

GRUPO: “A”

CARRERA: ING. EN SISTEMAS COMPUTACIONALES

CATEDRÁTICO: MCC. EDUARDO GENNER ESCALANTE

FECHA DE ENTREGA: 9/10/2020

CONCEPTOS BÁSICOS DE SEGURIDAD DE RED

Las definiciones son buenas como declaraciones de intenciones de alto nivel. ¿Cómo planeas implementar esa visión? Stephen Northcutt escribió una introducción a los conceptos básicos de la seguridad de la red durante más de una década atrás CSOonline, nosotros nos fijamos en tres fases de la seguridad de la red que deberían ser el marco de referencia base para su estrategia.

Métodos de seguridad de red: Para implementar este tipo de defensa en profundidad, hay una variedad de técnicas especializadas y tipos de seguridad de red.

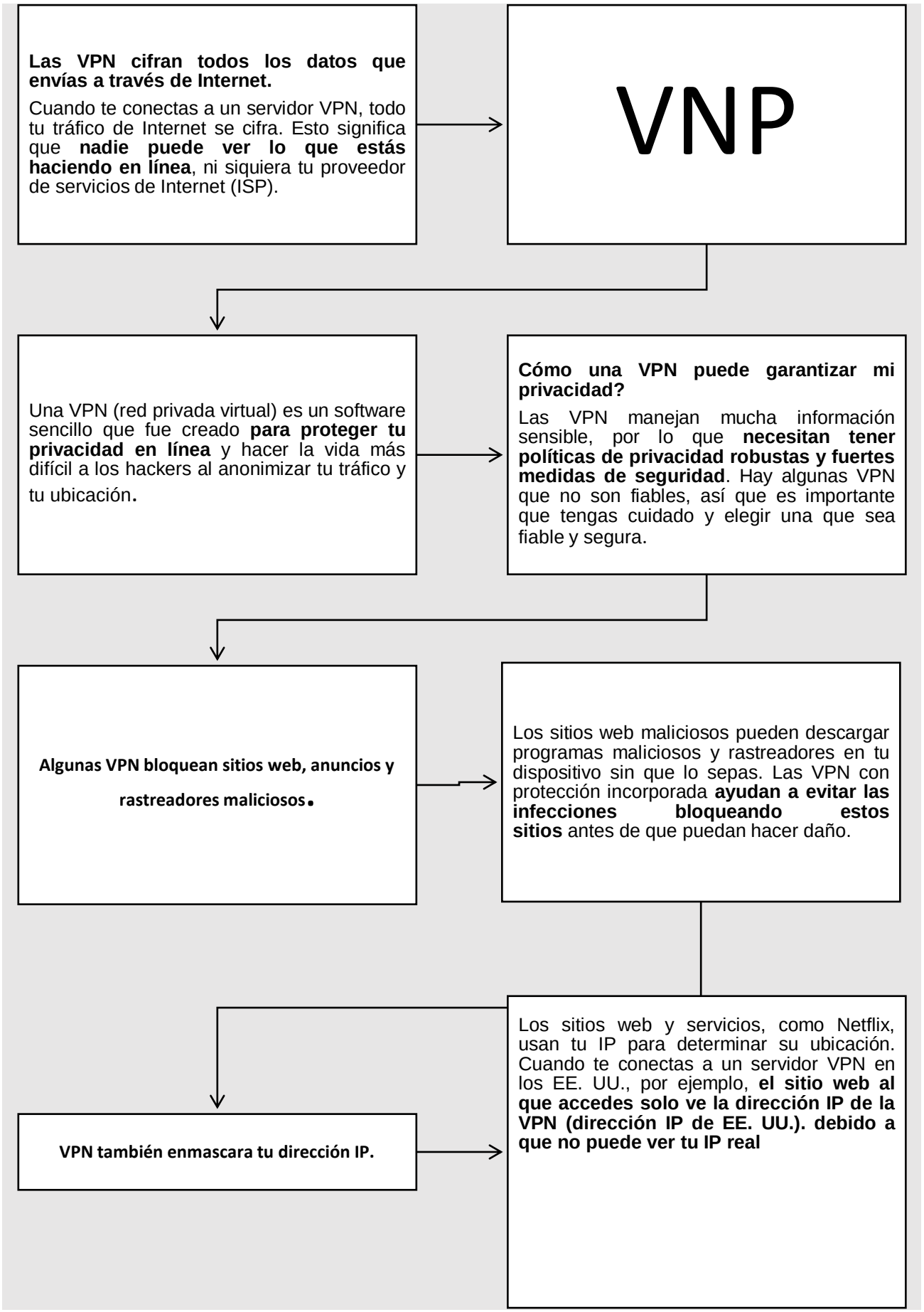
Seguridad de la red y la nube: Cada vez más empresas están desconectadas. cargando algunas de sus necesidades de cómputo a proveedores de servicios en la nube, creando infraestructuras híbridas donde su propia red.

Software de seguridad de red: Para cubrir todo ese base, necesitará una variedad de herramientas de software y hardware en su kit de herramientas. Lo mejor son un elemento en su estrategia híbrida de defensa en profundidad. Algunas de estas herramientas son productos corporativos de grandes proveedores, mientras que otras vienen en la forma de utilidades

Seguridad de la aplicación:

su red suele acceder a las aplicaciones no seguras. Debe usar hardware, software y procesos de seguridad para bloquear esas aplicaciones.

Seguridad del correo electrónico: el phishing es una de las formas más comunes de obtener acceso a una red. Las herramientas de seguridad de correo electrónico pueden bloquear tanto los mensajes entrantes como los salientes con datos confidenciales.


Las VPN cifran todos los datos que envías a través de Internet.
Cuando te conectas a un servidor VPN, todo tu tráfico de Internet se cifra. Esto significa que nadie puede ver lo que estás haciendo en línea, ni siquiera tu proveedor de servicios de Internet (ISP).
VNP
Una VPN (red privada virtual) es un software sencillo que fue creado para proteger tu privacidad en línea y hacer la vida más difícil a los hackers al anonimizar tu tráfico y tu ubicación.
Cómo una VPN puede garantizar mi privacidad?
Las VPN manejan mucha información sensible, por lo que necesitan tener políticas de privacidad robustas y fuertes medidas de seguridad. Hay algunas VPN que no son fiables, así que es importante que tengas cuidado y elegir una que sea fiable y segura.
Algunas VPN bloquean sitios web, anuncios y rastreadores maliciosos.
Los sitios web maliciosos pueden descargar programas maliciosos y rastreadores en tu dispositivo sin que lo sepas. Las VPN con protección incorporada ayudan a evitar las infecciones bloqueando estos sitios antes de que puedan hacer daño.
VPN también enmascara tu dirección IP.
Los sitios web y servicios, como Netflix, usan tu IP para determinar su ubicación. Cuando te conectas a un servidor VPN en los EE. UU., por ejemplo, el sitio web al que accedes solo ve la dirección IP de la VPN (dirección IP de EE. UU.). debido a que no puede ver tu IP real

Proxy: Los servidores proxy generalmente se usan como un puente entre el origen y el destino de una solicitud

un servidor proxy En este caso, el proxy puede cumplir algunas de las siguientes funciones:

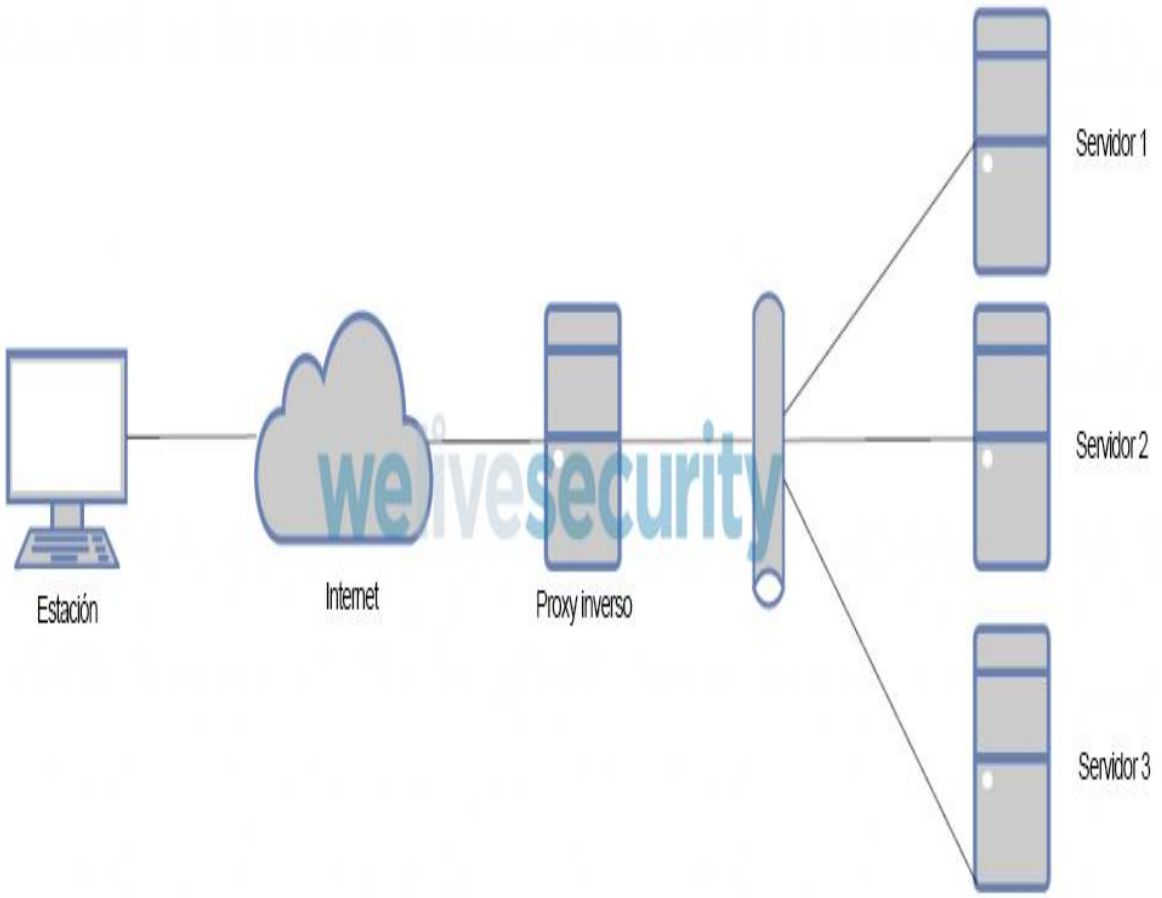
Control de acceso: es posible que los administradores del servidor proxy permitan que ciertos usuarios tengan o no acceso a Internet a través de restricciones en su propio inicio de sesión o direcciones IP, proporcionando al entorno una capa adicional de protección.

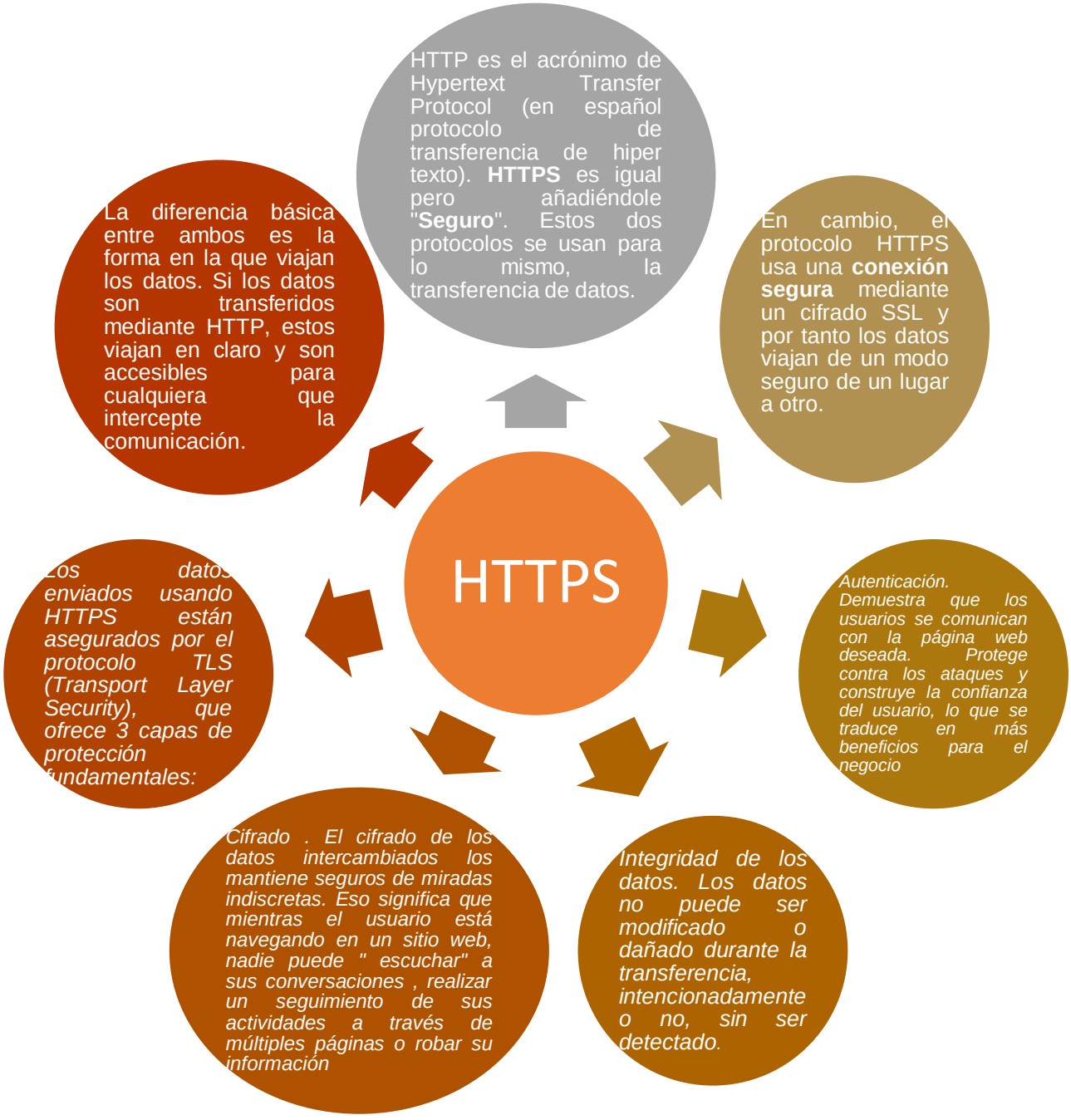
Filtrado de contenido: al estar en el medio del camino, el servidor también permite, o no, el acceso a ciertos sitios. Entre las reglas que se pueden aplicar están aquellas para bloquear sitios web específicos, pudiendo llegar a bloquear categorías completas.

Proxy inverso

Otro uso muy común son los servidores de proxy inverso. En los ejemplos anteriores, el origen de la conexión siempre estuvo dentro de la red, pasaba por el proxy hasta Internet. En el caso del proxy inverso, el origen de las solicitudes está en Internet y busca acceder a un servidor dentro del entorno.

EJEMPLO DE PROXY




HTTPS
HTTP es el acrónimo de Hypertext Transfer Protocol (en español protocolo de transferencia de hiper texto). **HTTPS** es igual pero añadiéndole "**Seguro**". Estos dos protocolos se usan para lo mismo, la transferencia de datos.
La diferencia básica entre ambos es la forma en la que viajan los datos. Si los datos son transferidos mediante HTTP, estos viajan en claro y son accesibles para cualquiera que intercepte la comunicación.
En cambio, el protocolo HTTPS usa una **conexión segura** mediante un cifrado SSL y por tanto los datos viajan de un modo seguro de un lugar a otro.
Los datos enviados usando HTTPS están asegurados por el protocolo TLS (Transport Layer Security), que ofrece 3 capas de protección fundamentales:
Autenticación. Demuestra que los usuarios se comunican con la página web deseada. Protege contra los ataques y construye la confianza del usuario, lo que se traduce en más beneficios para el negocio
Cifrado . El cifrado de los datos intercambiados los mantiene seguros de miradas indiscretas. Eso significa que mientras el usuario está navegando en un sitio web, nadie puede " escuchar" a sus conversaciones , realizar un seguimiento de sus actividades a través de múltiples páginas o robar su información
Integridad de los datos. Los datos no puede ser modificado o dañado durante la transferencia, intencionadamente o no, sin ser detectado.

EL robo de identidad ocurre cuando alguien hurta sus datos personales para cometer fraudes.

El ladrón de identidad puede usar esa información para solicitar un crédito, presentar declaraciones de impuestos o conseguir servicios médicos de manera fraudulenta. Estas acciones pueden dañar su buen nombre y su crédito, además de costarle tiempo y dinero para repararlo.

ROBO DE IDENTIDAD

Tipos de robo de identidad

Robo de identidad tributaria o relacionado con los impuestos: alguien utiliza su número de Seguro Social para presentar declaraciones falsas de impuestos federales o estatales.

Robo de identidad médica: alguien roba su identificación o tarjeta de Medicare, o su número de miembro del seguro médico. Los estafadores utilizan esta información para acceder a servicios médicos o enviar facturas falsas a su aseguradora.

Robo de identidad social: alguien utiliza su nombre y fotos para crear un perfil falso en las redes sociales.