1. **DESCRIPCIÓN DEL PROYECTO**
   1. Nombre del Proyecto:

Protección perimetral de Laboratorio de Bioinformática y Biología molecular de la UPCH.

* 1. Ámbito del Proyecto:

El proyecto abarca tanto la implementación hardware y software de la seguridad perimetral del Laboratorio, como el personal requerido para este.

* 1. Escenario inicial:

El Laboratorio de bioinformática cuenta con un centro de cómputo de 15 unidades, un clúster en sistema BLADE, servidores redundantes y DHCP, 69 artículos científicos y diversos premios/reconocimientos.

Oportunidad de mayor apoyo por parte del estado e instituciones privadas a la salud pública.

A pesar de esto, carece en seguridad informática y profesionales capacitados en el tema.

La burocracia y el deterioro de los equipos amenazan el buen funcionamiento de la institución.

* 1. Requerimientos del diseño:

Modernizar el hardware y software del Laboratorio.

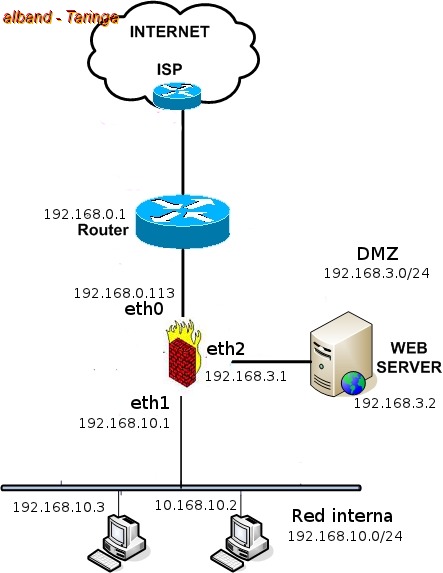
Deficiencia en seguridad informática.

* 1. Sistema de seguridad perimetral implantado:
* Cortafuegos, específicamente un proxy web (Squid).
* Servidores dedicados a la institución: servidor de base de datos, servidor web y un DMZ para el acceso de terceros verificados (opcional).
* N-IDS para monitorizar a los clientes ante una actividad anómala (opcional).
* Antivirus dedicado a detectar malware y spam la implantación.
  1. Diseño: La seguridad perimetral que vamos a establecer en el laboratorio es un modelo común como el siguiente:

Cada máquina-cliente está bajo una red interna que deriva en los servidores, las cuales serán de base de datos, de web y de red. Además del router que da salida hacia el internet, el Proxy será configurado en el servidor de red como también en cada máquina de los trabajadores.

Opcionalmente si el laboratorio lo desea podemos implementar un DMZ y N-IDS, para monitorear las máquinas, además de tener una mayor seguridad en el sistema de red.

Este diseño es referencial, pero nos muestra la manera en que serán conectadas las computadoras, servidores y maquinas necesarias para la seguridad perimetral del laboratorio. A nivel de software, el diseño clásico será implementado, con un servidor de red con sistema CentOS 7.0 y proxy Squid, un antivirus por definirse aún, además de software aplicativo para cada servidor y computadora, depende del uso que se les dará.



* 1. Planteamiento del problema
     1. Antecedentes
        1. Nacionales
* Informe de tesis en la Pontificia Universidad Católica del Perú: Diseño de una arquitectura de seguridad perimetral de una red de computadoras para una empresa pequeña.

Autor: Valenzuela Gonzales, Jorge Luis. Lima-Perú

* Informe de Tesis en la Universidad Nacional de Trujillo: Diseño de un modelo de red de zona perimetral segura para PYMES del Valle Jequetepeque.

Autor: Sánchez Quiroz, Bertha Natalí. Trujillo-Perú

* Informe de tesis en la Universidad de Lambayeque: Implementación de una solución de seguridad perimetral Open Source en La Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

Autores: Kenny Esleyther Ruiz Vieira. Wilson Delgado Ramos. Lambayeque-Perú.

* + - 1. Internacionales
* Informe de titulación en la Pontificia Universidad Católica de Ecuador: Análisis y diseño de un sistema de seguridad de red perimetral en la empresa Aseguradora del Sur – Matriz.

Autor: Bonilla Constante, Margarita Alejandra. Quito-Ecuador.

* Informe de Tesis en la ESPE: Implementación de un sistema de seguridad perimetral para las empresas Teamsourcing Cía. Ltda. Con software libre (ClearOS) y desarrollo de las políticas de seguridad basadas en el estándar ISO-27001.

Autor: Pilacuán Erazo, Edgar Rubén. Sangolquí-Ecuador

* Tesis Doctoral en la Universidad Ramón Lull de Barcelona: La Pre-historia de la Red

Autor: Andreu Veá I Baró. Barcelona-España

* + 1. Realidad problemática
       1. Diagnostico:

Cuenta con el Hardware básico necesario para brindar un correcto servicio, algo obsoleto y mal implementado; vulnerabilidad de la data y una falta de conocimiento del staff de trabajadores en el área de seguridad informática.

* + - 1. Pronostico:

Hardware y software actualizado, bien diseñado e implementado con una seguridad perimetral confiable.

* + - 1. Control del pronóstico:

Contrato de personal capacitado en seguridad informática, actualización ocasional de hardware/software y/o seguridad perimetral.

* 1. Objetivos
     1. Objetivo general:
* Diseñar e Implementar una seguridad perimetral en el Laboratorio de Bioinformática y Biología molecular usando un servidor proxy con Squid en plataforma Linux-CentOS con la finalidad de realizar un mejor manejo en la información de los servidores y evitar posibles amenazas externas.
  + 1. Objetivos específicos:
* Identificar problemas y oportunidades de mejora
* Análisis y diseño de un servidor proxy web.
* Actualización de hardware.
* Instalación y configuración del proxy en Squid en Linux-CentOS7.
* Realizar pruebas y corregir errores.
* Filtrar las diferentes solicitudes cliente-servidor.
  1. Justificación
     1. Técnica:
* Inspeccionar hardware de la empresa para su modernización.
* Trabajar en Sistema Linux.
  + 1. Operativa:
* No debe ser tan complejo a la hora de usarse, de manera que el staff no cause ningún problema a fallo en el sistema.
* Poder ser mejorable, debido a que las amenazas están en constante evolución, el servidor proxy debe también ser actualizado.
  + 1. Económica:
* Sin una seguridad perimetral bien implementada, el sistema es más vulnerable a ataques, muchas veces ocasionando más pérdidas por un ahorro en este ámbito.
* Es viable según un análisis de costo y beneficio.

|  |  |
| --- | --- |
| DESCRIPCIÓN | COSTO |
| RECURSOS HUMANOS  Programador en sistema de redes:  Ingeniero en redes:  Técnico en telecomunicaciones:  RECURSOS TEXNOLÓGICOS  Servidor Proxy:  Router TP.Link:  Switch:  4 Computadoras empresariales:  Insumos:  SERVICIOS  Internet de Negocios Movistar: | 400  4000  400  500  40  29  1848  30  101.3 |
| COSTO TOTAL | 7348.3 |

* 1. Limitaciones:
* Se trata de tomar un consenso en el presupuesto del proyecto con el Laboratorio de bioinformática (costo-beneficio), para ver si es una limitante.
* La burocracia al tratar de llegar a un acuerdo con el laboratorio.

1. **MARCO TEORICO**
   1. **Definiciones Teóricas**
      1. ¿Qué es un Servidor proxy?

Un servidor proxy es un equipo dedicado o un sistema de software que se ejecuta en un equipo de cómputo que actúa como intermediario entre un dispositivo de punto final, como una computadora, y otro servidor del cual un usuario o cliente solicita un servicio.

* + 1. Características del servidor:

**Filtrado**. Una de las principales características con la que cuenta un servidor proxy.

**Autenticación.** Si bien hablamos de que un proxy ayuda a incrementar la seguridad y a que los usuarios de la red no se salgan de los sitios permitidos.

**Almacenamiento de Logs**.Cómo nos podríamos dar cuenta de la navegación de los usuarios, si no fuera gracias al log. Con el log, tendremos en nuestro proxy, todas y cada una de las páginas que los usuarios de la re visitaron, sin excepción.

**Almacenamiento de Caché.** Posiblemente no sea un caché auténtico, pero lo que sí, es que un servidor proxy es capaz de guardar el contenido total de sitios web visitados, permitiendo que cuando alguien más ingrese al sitio, este pueda ser cargado de inmediato sin tener que realizar el llamado externo.

**Conexiones Compartidas.**

**Listas Negras**. ¿Qué pasa con un sitio web malicioso al que alguien ingresó desde una red proxy? Bueno, pues se va a la lista negra. Esta lista negra se conforma de todos los sitios a los que no estará permitido ingresar por distintas razones

**Bloqueo de IP.**

**Archivos no Permitidos**

**Control de Usuarios**

**Evita desvío de recursos. En ocasiones, la red u otros recursos de la empresa, pueden ser utilizados de forma indebida. Por ejemplo, para jugar algo desde la computadora.**

* + 1. **¿Qué es un Squid?**

**Squid es un popular programa de software libre que implementa un servidor proxy y un dominio para caché de páginas web, publicado bajo licencia GPL. Tiene una amplia variedad de utilidades, desde acelerar un servidor web, guardando en caché peticiones repetidas a DNS y otras búsquedas para un grupo de gente que comparte recursos de la red, hasta caché de web, además de añadir seguridad filtrando el tráfico. Está especialmente diseñado para ejecutarse bajo entornos tipo Unix. Squid ha sido desarrollado durante muchos años y se le considera muy completo y robusto. Aunque orientado a principalmente a HTTP y FTP es compatible con otros protocolos como Internet Gopher. Implementa varias modalidades de cifrado como TLS, SSL, y HTTPS.**

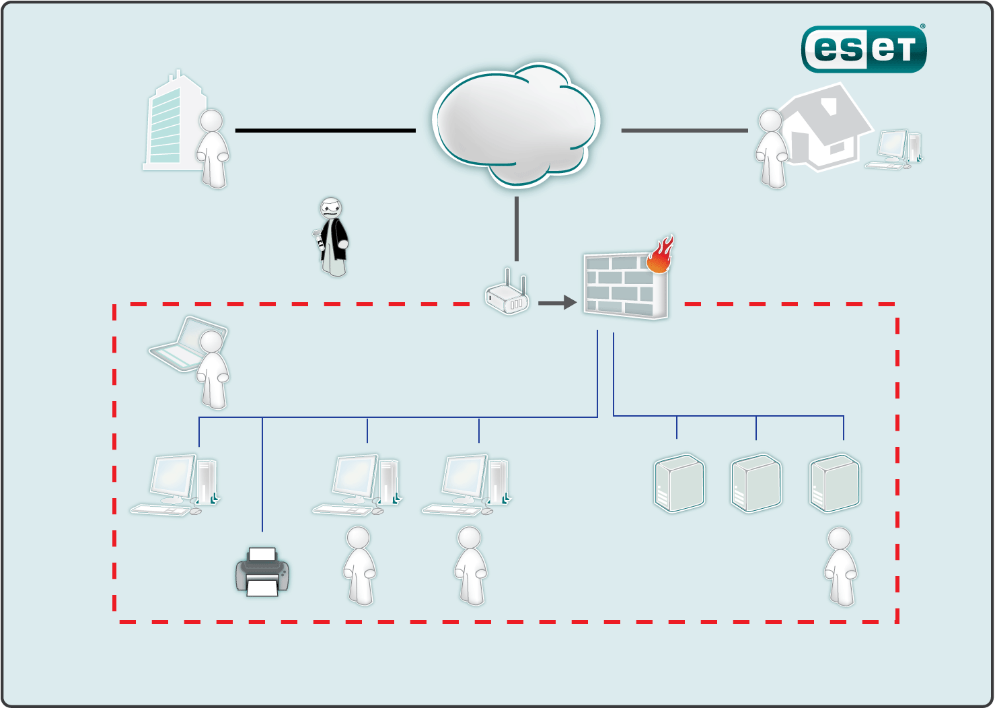
* + 1. **Beneficios:**

**Además del almacenamiento en caché, Squid ofrece una amplia variedad de funciones, como la distribución de la carga en las jerarquías de los servidores proxy, la definición de estrictas listas de control de acceso para todos los clientes que accedan al proxy, el permiso o la denegación de acceso a páginas Web concretas (con la ayuda de otras aplicaciones) y la generación de estadísticas de las páginas Web visitadas con más frecuencia con el fin de evaluar los hábitos de navegación de los usuarios. Squid no es un proxy genérico. Normalmente sólo ejerce sus funciones con conexiones HTTP.**

* + 1. **Perímetro de la red :**

**Durante muchos años, luego de la masificación del acceso a Internet, las redes corporativas basaron su seguridad en un modelo que consideraba el perímetro como principal barrera.**

**El perímetro está plasmado en el siguiente esquema de red, que será reconocido por muchos de los administradores de tecnología que leen este espacio y han diagramado la topología de su organización**



* **El perímetro (en el gráfico, la línea roja punteada) es la división tanto física como lógica entre lo que está dentro de la red y aquello que está fuera. Además de las barreras físicas, con el acceso a Internet las redes corporativas enfrentaron la obligación de controlar la entrada y salida de información de la empresa hacia y desde el ciberespacio. Y para ello, se utilizan una serie de dispositivos perimetrales (servidores proxy, router, firewalls) que permiten establecer controles de seguridad para la información que entra y sale de la red.**
  + 1. Redes privadas virtuales (VPN):

Es una red privada construida dentro de una infraestructura de red pública, que se utilizan para conectar de forma segura a un recurso de la red privada a los usuarios remotos a través de accesos a Internet proporcionados por ISP, en lugar de líneas dedicadas.

Por lo tanto, el sistema VPN brinda una conexión segura a un bajo costo, ya que todo lo que se necesita es el hardware de ambos lados de las redes conectadas. Sin embargo, no garantiza una calidad de servicio comparable con una línea dedicada, ya que la red física es pública y por lo tanto no está garantizada.

* + 1. Funcionamiento de una VPN:

A través de un VPN tunneling que crea un canal de comunicación dentro de una red de computadoras al usar la VPN se aplica una capa de cifrado y autentificación donde la información aunque esté pasando por intermediarios esta no será leída por terceros hasta la llegada de la información.

* + 1. Software y servicios Host Bastión:

Un host bastión es un equipo que está totalmente expuesto a los ataques. El sistema está en el lado público de la zona desmilitarizada (DMZ), protegidos por un firewall o un router de filtrado. Con frecuencia las funciones de estos sistemas son esenciales para el sistema de seguridad de la red. De hecho, los firewalls y routers pueden ser considerados los hosts de bastión.

Debido a su exposición, una gran cantidad de esfuerzo se debe poner en el diseño y la configuración de hosts bastión para reducir al mínimo las posibilidades de penetración. Otros tipos de hosts de bastión son la web, correo, DNS y servidores FTP. Algunos administradores de red también se utilizan como chivos expiatorios los hosts de baluarte, estos sistemas son expuestos deliberadamente a hackers potenciales tanto retraso y facilitar el seguimiento de los intentos de robos.

Los bastiones pueden clasificarse en tres tipos:

**1.-Single-homed bastión host:** Es un dispositivo con una interfaz única de red, frecuentemente se utiliza para una puerta de enlace en el nivel de aplicación. El router externo está configurado para enviar los datos al Bastión Host y los clientes internos enviar los datos de salida al host. Finalmente el host evaluará los datos según las directrices de seguridad.

**2.-Dual-homed bastión host:** Es un dispositivo que tiene al menos dos interfaces de red. Sirve como puerta de enlace al nivel de aplicación y como filtro de paquetes. La ventaja de usar este host es crear un quiebre entre las red externa e interna, lo que permite que todo el tráfico de entrada y salida pase por el host. Este host evitará que un hacker intenté acceder a un dispositivo interno.

**3.-Multihomed bastión host:** Un Bastión host interno puede ser clasificado como multihomed. Cuando la política de seguridad requiere que todo tráfico entrante y salida sea enviado a través de un servidor proxy, un nuevo servidor proxy debería ser creado para la nueva aplicación streaming. Cuando se utiliza un bastión host como interno, debe residir dentro de una organización de la red interna, en general como puerta de acceso para recibir todo el tráfico de un bastión host externo. Lo que agrega un nivel mayor de seguridad.

* + 1. Zonas desmilitarizadas (DMZ) y subredes controladas:

La zona desmilitarizada y subred controlada son pequeñas porciones de la red con servicios accesibles desde el exterior, sus diferencias son:

**Zona desmilitarizada:** Situada delante del cortafuegos, tras el router frontera.

**Red controlada:** Situada tras el cortafuegos.

Una zona desmilitarizada (DMZ) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa, es decir: los equipos locales (hosts) en la DMZ no pueden conectar con la red interna.

Los servidores en la DMZ se denominan "anfitriones bastión" ya que actúan como un puesto de avanzada en la red de la compañía.

\*El tráfico de la red externa a la DMZ está **autorizado**

\*El tráfico de la red externa a la red interna está **prohibido**

\*El tráfico de la red interna a la DMZ está **autorizado**

\*El tráfico de la red interna a la red externa está **autorizado**

\*El tráfico de la DMZ a la red interna está **prohibido**

\*El tráfico de la DMZ a la red externa está **denegado**

**Subredes controladas o Screened subnet**

\*Es la arquitectura más segura, pero también la más compleja; se utilizan dos routers, denominados exterior e interior, conectados ambos a la red perimétrica.

\*En esta red perimétrica, que constituye el sistema cortafuegos, se incluye el host bastión y también se podrían incluir sistemas que requieran un acceso controlado, como baterías de módems o el servidor de correo, que serán los únicos elementos visibles desde fuera de nuestra red.

\*El router exterior tiene como misión bloquear el tráfico no deseado en ambos sentidos (hacia la red perimétrica y hacia la red externa), mientras que el interior hace lo mismo pero con el tráfico entre la red interna y la perimétrica: así, un atacante habría de romper la seguridad de ambos routers para acceder a la red protegida; incluso es posible implementar una zona desmilitarizada con un único router que posea tres o más interfaces de red, pero en este caso si se compromete este único elemento se rompe toda nuestra seguridad, frente al caso general en que hay que comprometer ambos, tanto el externo como el interno.

* + 1. Antivirus:

Un antivirus es una aplicación que trata de detectar y eliminar los virus informáticos, es decir, aquellos programas maliciosos que pueden ingresar en un ordenador y producir daños tales como la pérdida de efectividad del procesador, la supresión de archivos, la alteración de datos, la exposición de información confidencial a usuarios no autorizados o la desinstalación del sistema operativo. Para mantener nuestros computadores a salvo,[existe una variada oferta de antivirus.](http://www.valortop.com/mejor-antivirus)

* + 1. Proxy Cache Web :

Un servidor proxy o también llamado caché web, es un equipo dentro de la red que recibe solicitudes HTTP en nombre de un servidor web de origen. La caché consiste en almacenar los objetos que han sido solicitados por el cliente recientemente.

* + 1. Antivirus de navegación :

Al navegar por internet, descargar archivos o recibir mails entre otras tareas online se genera inseguridad para tu ordenador y todo lo que esté en él. El antivirus informático ayuda a proteger el equipo y evitar que se pueda perder información importante

* + 1. Servidores de DNS:

Un Servidor DNS en informática responde a las siglas Domain Name System. Gracias a los servidores DNS conocemos los nombres en las redes, como las de Internet o las de una red privada. Es decir, conocemos la dirección IP de la máquina donde está alojado el dominio al que vamos a acceder.

* + 1. Servidores RADIUS:

Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

Cuando se realiza la conexión con un ISP mediante [módem](https://es.wikipedia.org/wiki/Módem), [DSL](https://es.wikipedia.org/wiki/Asymmetric_Digital_Subscriber_Line), [cablemódem](https://es.wikipedia.org/wiki/Cablemódem), Ethernet o [Wi-Fi](https://es.wikipedia.org/wiki/Wi-Fi), se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo Network Access Server (NAS) sobre el protocolo [PPP](https://es.wikipedia.org/wiki/Point-to-Point_Protocol), quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como [PAP](https://es.wikipedia.org/wiki/Password_Authentication_Protocol), CHAP o [EAP](https://es.wikipedia.org/wiki/Extensible_Authentication_Protocol). Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como [L2TP](https://es.wikipedia.org/wiki/L2TP), etc.

* + 1. Servidor de NTP :

Es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la latencia variable.

* + 1. Gestor de ancho de banda:

Es una potente herramienta que mide la cantidad de ancho de banda que se usa en una red. Este gestor del ancho de banda para Windows se puede configurar rápida y fácilmente para leer los datos de tráfico de su router, que luego se mostrarán en gráficos claros y completos. Con este gestor del ancho de banda, puede evaluar la actividad actual de la red al igual que consultar los históricos de datos transferidos en los últimos 14 días o 12 meses.

* + 1. Sistema de monitorización de equipos:

Los sistemas de monitorización se encargan de supervisar la tecnología que utiliza una empresa (hardware, redes y comunicaciones, sistemas operativos o aplicaciones, entre otros) con el fin de analizar su funcionamiento y su rendimiento, y de detectar y alertar acerca de posibles errores. Un buen sistema de monitorización es capaz de monitorizar **dispositivos, infraestructuras, aplicaciones, servicios, e incluso procesos de negocio**.

* + 1. Sistemas de realización de backups:

Los **sistemas de** backup en la empresa cumplen una función fundamental y no es otra que la salvaguarda de los datos más importantes que se generan en los procesos de la compañía durante su día a día.

* + 1. Bastionado de equipos:

Tiene como objetivo la correcta implantación de políticas de seguridad, endurecimiento y delimitación clara los privilegios de usuarios, grupos, roles y configuración de servicios. Active Directory, LDAP, Fortificación de contraseñas, Firewall, DMZ entre otras.

* 1. **Cortafuegos**
     1. Definición:
        + - Un cortafuegos es una máquina segura y confiable que se asienta entre una red privada y una red pública. La máquina cortafuegos se configura con un conjunto de reglas que determinan a qué tráfico de red se le permitirá pasar y cuál será bloqueado o rechazado. En algunas organizaciones grandes, puede que encuentre un cortafuegos localizado dentro de la red corporativa para separar áreas sensibles de la organización de otros empleados. Algunos casos de criminalidad informática acontecen dentro de la misma organización, no sólo provienen de fuera.
     2. Cortafuegos (firewalls):
* Un cortafuego (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.
* Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

**Las funciones principales de un firewall son:**

1.-control de acceso

2.-Traslación de direcciones

3.-Autentificación

4.-Balanceo de Contenido

5.-Seguridad de Contenido

6.-Encriptación (para permitir establecer VPN’s en el Internet)

* + 1. Sistemas de Detección de Intrusos (IDS):

Es un sistema para monitorizar los eventos que ocurren en un sistema informático, o escucha el tráfico en la red para detectar actividades sospechosas, y accesos no autorizados a un sistema u ordenador de una red; y de este modo, reducir el riesgo de intrusión. Existen dos tipos de sistemas de detección de intrusos:

\***N-IDSes (basados en red):** Un IDS basado en red monitoriza los paquetes que circulan por nuestra red en busca de elementos que denoten un ataque contra alguno de los sistemas ubicados en ella; el IDS puede situarse en cualquiera de los hosts o en un elemento que analice todo el tráfico (como un HUB o un enrutador)

\***H-IDSes (basados en host):** Mientras que los sistemas de detección de intrusos basados en red operan bajo todo un dominio de colisión, los basados en máquina realizan su función protegiendo un único sistema; de una forma similar - guardando las distancias, por supuesto - a cómo actúa un escudo antivirus residente en MS-DOS, el IDS es un proceso que trabaja en background (o que despierta periódicamente) buscando patrones que puedan denotar un intento de intrusión y alertando o tomando las medidas oportunas en caso de que uno de estos intentos sea detectado.

* + 1. Cortafuegos vs IDS :

La principal diferencia es que el firewall realiza acciones reales, como el bloqueo y el filtrado, mientras que IDS solo detecta y alerta al administrador del sistema

* + 1. Configuraciones:

**Conexiones:** El primer paso en la definición de una regla de firewall es determinar qué se debe hacer con una conexión que cumple con los criterios que define la regla.

**Equipos:** Especifique los equipos a los cuales se debe aplicar la regla:

**Comunicaciones:** El paso final en la creación de una nueva regla de firewall es definir los protocolos de comunicaciones usados para la conexión. Puede especificar estos protocolos:

TCP, UDP, TCP y UDP, ICMP, ICMPv6 o todos

* + 1. Cortafuego del proveedor externo:

Una de las circunstancias a las que nos vamos a enfrentar, y que muchas veces nos olvidamos, es la existencia de gran cantidad de proveedores dentro de las organizaciones industriales. Las mismas recurren a productos y servicios especializados de terceros que luego deben ser soportados durante su ciclo de vida y garantizar así un respaldo en caso de incidencias.

* + 1. Modos de operación
    2. Configuración de interfaces vlan:

Siempre que los host en una VLAN necesitan comunicarse con host en otra VLAN, debe rutearse el tráfico entre ellos. Esto se conoce como ruteo InterVLAN. En los switches de Catalyst es lograda por la creación de las interfaces de la capa 3 (interfaces virtuales del Switch (SVI)).

* + 1. Configuración de interfaces físicas:

Active la interfaz: de manera predeterminada, las interfaces LAN y WAN no están activadas. La interfaz se debe activar mediante el comando no shutdown. Es como encender la interfaz. La interfaz también debe estar conectada a otro dispositivo para que la capa física esté activa.

* + 1. Acceso remoto

Acceso remoto mediante el puerto SSH.

* 1. **Sistemas Operativos**
     1. Linux:

Es un sistema operativo libre [tipo Unix](https://es.wikipedia.org/wiki/Unix-like); [multiplataforma](https://es.wikipedia.org/wiki/Multiplataforma), multiusuario y [multitarea](https://es.wikipedia.org/wiki/Multitarea). El sistema es la combinación de varios proyectos, entre los cuales destacan GNU (encabezado por Richard Stallman y la [Free Software Foundation](https://es.wikipedia.org/wiki/Free_Software_Foundation)) y el núcleo [Linux](https://es.wikipedia.org/wiki/Núcleo_Linux)(encabezado por [Linus Torvalds](https://es.wikipedia.org/wiki/Linus_Torvalds)). Su desarrollo es uno de los ejemplos más prominentes de [software libre](https://es.wikipedia.org/wiki/Software_libre): todo su fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera, bajo los términos de la GPL ([Licencia Pública General de GNU](https://es.wikipedia.org/wiki/GPL)) y otra serie de licencias libres.

* + 1. Ventajas de uso:

\*Linux es muy robusto, estable y rápido: Ideal para servidores y aplicaciones distribuidas. A esto se añade que puede funcionar en máquinas humildes: Linux puede correr servicios en un x86 a 200 MHz con calidad

\*Linux es libre: Esto implica no sólo la gratuidad del software, sino también que Linux es modificable y que Linux tiene una gran cantidad de aplicaciones libres en Internet. Todo ello arropado por la inmensa documentación de Linux que puede encontrarse en la Red

\*Linux ya no está restringido a personas con grandes conocimientos de informática: Los desarrolladores de Linux han hecho un gran esfuerzo por dotar al sistema de asistentes de configuración y ayuda, además de un sistema gráfico muy potente. Distribuciones Linux como Red Hat/Fedora tienen aplicaciones de configuración similares a las de Windows.

* + 1. Desventajas:

\*Windows es incompatible con Linux: Este punto es difícil de explicar: no quiere decir que no podamos tener instalados ambos Sistemas (que es relativamente fácil de hacer)

Uno de los problemas es que desde Windows no podremos escribir en particiones Linux o que desde Linux no podremos escribir (en sentido amplio) en particiones NTFS (Windows XP, 2000...) aunque esto último se está investigando,

\*En la mayoría de distribuciones Linux hay que conocer nuestro Hardware a la hora de instalar

* 1. **Intranet y Extranet**
     1. Red:

Red de computadoras. Como en todo proceso de comunicación, se requiere de un emisor, un mensaje, un medio y un receptor. ... Un ejemplo es Internet, el cual es una gran red de millones de ordenadores ubicados en distintos puntos del planeta interconectados básicamente para compartir información y recursos.

* + 1. Internet:

Un conjunto descentralizado de [redes de](https://es.wikipedia.org/wiki/Red_de_telecomunicación) [comunicación](https://es.wikipedia.org/wiki/Red_de_telecomunicación) interconectadas que utilizan la familia de protocolos TCP/IP, lo cual garantiza que las redes físicas heterogéneas que la componen formen una red lógica única de alcance mundial.

* + 1. Intranet:

Es una red informática que utiliza la tecnología del protocolo de Internet para compartir información, [sistemas operativos](https://es.wikipedia.org/wiki/Sistemas_operativos) o servicios de computación dentro de una organización. Suele ser interna, en vez de pública como [internet](https://es.wikipedia.org/wiki/Internet), por lo que solo los miembros de esa organización tienen acceso a ella.

* + 1. Extranet:

Es una red privada que utiliza protocolos de Internet, protocolos de comunicación y probablemente infraestructura pública de comunicación para compartir de forma segura parte de la información u operación propia de una organización con proveedores, compradores, socios, clientes o cualquier otro negocio u organización. Se puede decir en otras palabras que una extranet es parte de la Intranet de una organización que se extiende a usuarios fuera de ella, usualmente utilizando Internet y sus protocolos.

* 1. **Infraestructura de la Tecnología de Información y Seguridad**
     1. Políticas y Procedimientos de Seguridad:
* Las políticas son instructivos que indican un predeterminado curso de acción, una manera de manejar situaciones o problemas. Son declaraciones generales que proveen una guía a los empleados que deban tomar decisiones tales como: identificación y control de acceso, respaldo de datos, planes de contingencia y detección de intrusos.
* Las políticas no son procedimientos, aunque en ambos casos se requiera estricto cumplimiento. A diferencia de estas, los procedimientos provén métodos específicos para hacer las cosas.
  + 1. Seguridad física y del entorno:

Son las medidas que se deben adoptar para salvaguardar tanto los equipos (hardware) como las instalaciones de la organización, tales como:

-Control del personal que accede a los distintos recursos y dependencias.

- sistemas de alarma, etc.

* + 1. Seguridad perimetral:

El perímetro es el punto o conjunto de puntos de la red interna de confianza gestionada por la organización en contacto con otras redes externas no fiables. Los intrusos poseen acceso a los servicios ofrecidos o accesibles desde el exterior.

Las medidas adoptadas para proteger el perímetro son instalando cortafuegos, redes privadas virtuales, routers bien configurados, antivirus, etc.

* + 1. Seguridad de red propiamente dicha:

Mecanismos adoptados ante el acceso no autorizado a la red interna de la organización como:

-Segmentación de redes mediante routers y switches.

-Añadir cifrados durante el transporte de datos.

* + 1. Seguridad de equipos:

La seguridad de equipos tanto servidores como clientes implican:

-Mantener actualizados los parches de seguridad.

-Antivirus activo

El mayor riesgo ocurre cuando el atacante puede acceder al equipo a través de vulnerabilidades en servicios del sistema operativo.

El bastionado y la aplicación de plantillas de seguridad constituyen las dos herramientas básicas para proteger equipos.

* + 1. Seguridad de aplicaciones:

Las aplicaciones se protegen realizando un control de acceso mediante la sólida implantación de mecanismos de autenticación y autorización. Una medida de seguridad adicional consiste en la instalación de cortafuegos de aplicación, dedicados a filtrar el tráfico específico de distintas aplicaciones como correo (SMTP), web (http), base de datos, etc.

* + 1. Seguridad de datos:

Si un atacante ha traspasado todas las barreras anteriores y posee acceso a la aplicación; la autenticación y la autorización, junto con el cifrado, constituyen las tecnologías más empleadas para proteger los datos.

* 1. **Tipo de Seguridad**

2.2.1.Seguridad física:

La seguridad física está relacionada con los recursos y el espacio físico utilizados para la protección de los elementos que conforman los sistemas de información dentro de la empresa, tales como:

* Control de acceso físico a servidores y cuarto de control.
* Ubicación y ambiente adecuado de los servidores y cuarto de control.
* Uso correcto de PC’s

2.2.2. Seguridad lógica:

La seguridad lógica está relacionada con los procedimientos y recursos lógicos utilizados para proteger los sistemas de información dentro de la empresa. Tales como:

* Creación de perfiles de usuarios, i.e, el acceso a la información será parcial dependiendo el perfil del usuario y utilizando contraseñas.
* Algoritmos de encriptación para la transmisión de información.
* Sistemas de monitoreo para llevar un control sobre el acceso a los sistemas y usuarios.
  1. **Propiedades de la Seguridad Informática**
     1. Autenticidad:

Garantiza que una entidad es quien dice ser. El servicio de autenticidad protege contra la suplantación de personalidad (masquerade), es decir, cuando una entidad externa se hace pasar por quien no es. Este servicio puede ser utilizado de 2 formas: autenticación de una de las partes (origen o destino), o autenticación mutua.

* + 1. Integridad:

El objetivo de esta propiedad es garantizar que los datos y recursos no hayan sido alterados y sean fiables. Asegura al receptor que el mensaje recibido fue el mismo que el enviado por el emisor, es decir, la información no fue añadida, modificada o sustraída. Un ataque a esta propiedad puede darse en el almacenamiento, transporte o procesamiento de la información.

* + 1. Disponibilidad:

Tiene como objetivo garantizar que la información y los servicios no sean interrumpidos y permanezcan accesibles en forma permanente.

* + 1. Confiabilidad:

Garantiza que el mensaje no sea revelado a terceras personas o no autorizadas, pero que si sean entendibles por el destinatario correcto.

* 1. **Vulnerabilidad en Intranet y/o Extranet**
     1. Tipos de vulnerabilidades:

Físicas.- Se relaciona con el espacio donde se encuentran ubicados los dispositivos de red; por ejemplo:

-Inadecuadas instalaciones de trabajo

-Disposición desorganizada de cables de energía y red

-Ausencia de recursos para combatir incendios, etc.

En Hardware.- Son vulnerabilidades de hardware las que se relacionan con los componentes de hardware de la red. Por ejemplo:

-Equipos inadecuados para su uso

-Falta de equipos para plan de contingencia

-Defectos de fabricación de los dispositivos, etc.

En Software.- Están relacionadas con las aplicaciones de sistemas informáticos. Por ejemplo:

-Mala instalación de aplicaciones por usuarios inexpertos o malintencionados

-Configuraciones incompletas, etc.

En la transmisión de la información.- Existen vulnerabilidades en la transmisión de información debido a:

-Ausencia de sistemas de encriptación

-Sistema inadecuado para envío de mensajes de alta prioridad

-Errores en los medios de transmisión

* + 1. Amenazas:

Naturales.- Estas amenazas son relacionadas con las condiciones naturales. Por ejemplo: la humedad, el clima, desastres naturales, etc. Pueden ser prevenidas ubicando bien el entorno de los equipos de red.

Accidentales o Involuntarias.- Aparecen en forma no premeditada. Por ejemplo:

-Operaciones indebidas de usuarios inexpertos

-Bugs o fallos en el software

-Funcionamiento irregular de los sistemas, etc.

Intencionales.-Estas amenazas son la participación maliciosa de un sujeto o entidad para un uso indebido de la red. Las amenazas intencionales se denominan ataques.

* + 1. Ataques:

Un ataque informático es la violación de la seguridad de una red (confidencialidad, integridad, disponibilidad o uso legítimo).

La información que circula por la intranet o extranet de una empresa puede ser atacada de formas como:

-Interrupción o Denegación de servicio.- El intruso bloquea la transmisión de la información para que el receptor no la reciba. Este ataque afecta el principio de disponibilidad de la información.

-Intercepción.- El emisor transmite la información al receptor, pero esta es interceptada por terceros. También puede realizarse la divulgación o repetición del contenido. Este ataque afecta al principio de confidencialidad.

-Suplantación de identidad.- El intruso se hace pasar por el emisor generando información y transmitiéndola al receptor. Este ataque permite el acceso a la información a personas no autorizadas. Por ejemplo, cuando una persona o entidad suplanta la identidad de la otra, se enmascara para realizar una función no autorizada en la red. Afecta al principio de autenticidad de la información.

-Modificación.- El intruso intercepta la información enviada por el emisor, la altera o modifica (sustracción o adición del mensaje) y la transmite al receptor. Afecta el principio de integridad.

* + 1. Intrusos:

Existen 2 clases de intrusos:

Pasivo.- El intruso pasivo accede a la información confidencial que está siendo transmitida sin realizar ninguna modificación en ella, es decir, se dedica a monitorear la red. Los objetivos principales son la intercepción de la información y el análisis de tráfico.

Este intruso es muy difícil de detectar porque no ocasiona ninguna alteración a la información; sin embargo, se puede prevenir un ataque de este tipo con mecanismos de cifrado.

Activos.- El intruso activo a diferencia del pasivo altera la información interceptada.

Este tipo de intrusos puede ser:

Terroristas.- Es decir, cualquier persona que ataca al sistema para causar algún daño en él. ´por ejemplo, borrar bases de datos o destruir sistemas de ficheros, etc.

Exempleados.- Personas, descontentas con la organización que pueden aprovechar debilidades de un sistema que conocen. Por ejemplo: insertar troyanos, bombas lógicas o simplemente conectarse al sistema como si aún trabajaran para la empresa.

* 1. **Metodología para el Diseño de Seguridad en Redes Int-Extranet**
     1. Análisis de riesgo:

Una evaluación efectiva de riesgos en la seguridad de la información considera tanto los  temas organizacionales como los técnicos, examina cómo la gente emplea la infraestructura  en forma diaria. La evaluación es de vital importancia para cualquier iniciativa de mejora en  seguridad, porque genera una visión a lo ancho de la organización de los riesgos de seguridad de la información, proveyéndonos de una base para mejorar a partir de allí.

Como referencia podemos ver la metodología OCTAVE, el núcleo central de OCTAVE es un conjunto de criterios (principios, atributos y resultados) a partir de los cuales se pueden desarrollar diversas metodologías.

**Objetivos**

* Desmitificar la falsa creencia: La Seguridad Informática es un asunto meramente técnico
* Presentar los principios básicos y la estructura de las mejores prácticas internacionales que guían los asuntos no técnicos.

**Activos**

OCTAVE divide los activos en dos tipos que son:

* Sistemas (Hardware. Software y Datos)
* Personas

**Fases**

La metodología OCTAVE está compuesta en tres fases:

* Visión de organización: Donde se definen los siguientes elementos: activos, vulnerabilidades de organización, amenazas, exigencias de seguridad y normas existentes.
* Visión tecnológica: se clasifican en dos componentes o elementos: componentes claves y vulnerabilidades técnicas.
* Planificación de las medidas y reducción de los riesgos: se clasifican en los siguientes elementos: evaluación de los riesgos, estrategia de protección, ponderación de los riesgos y plano de reducción de los riesgos.
  + 1. Diseño de seguridad:

El diseño de seguridad de red tanto físico como lógico, tomamos como referencia la metodología SAFE para pymes.

Safe no es una guía para diseñar redes, sino una guía para asegurar redes, ya que ellas seguirán ofreciendo todos los servicios que el usuario espera de la red.

La metodología Safe se basa en un enfoque modular por 2 motivos importantes.

-La arquitectura relaciona la seguridad entre los distintos bloques funcionales de la red.

-Permitir al diseñador evaluar e implementar la seguridad, módulo a módulo, en lugar de hacerlo generalmente.

* + 1. Manual de políticas:

Para el Manual de políticas y procedimientos se toma como guía la NORMA ISO 17799, tanto para la seguridad física como la lógica de la red, que trata de promover sistemas de calidad para la seguridad del usuario inclinándose al conocimiento y a la aplicación de la normalización como base de la calidad.

1. **IMPLEMETACION**
   1. **Normas, Políticas y Procedimientos de Seguridad**
      1. Normas Internaciones de seguridad informática:
      * ISO 17799 define la informacióncomo un activo que posee valor para la organización y requiere por tanto de una protección adecuada. El objetivo de la seguridad de la informaciónes proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

La norma ISO/IEC 17799 establece 10 dominios de control:

1. Política de seguridad

2. Aspectos organizativos para la seguridad.

3. Clasificación y control de activos

4. Seguridad ligada al personal

5. Seguridad física y del entorno

6. Gestión de comunicaciones y operaciones.

7. Control de accesos.

8. Desarrollo y mantenimiento de sistemas.

9. Gestión de continuidad de negocio.

10. Conformidad con la legislación.

* + - A semejanza de otras normas ISO, ISO/IEC 27000 es un conjunto de estándares desarrollados o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.
    - La norma ISO/IEC 27000: Vocabulario estándar para el sistema de gestión de seguridad de la información (SGSI) para todas las normas de la familia.
    - La norma ISO/IEC 27001:Consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.
    - La norma ISO/IEC 27002:Es código de buenas prácticas para la gestión de seguridad de la información.
    - La norma ISO/IEC 27003: son directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001.
    - La norma ISO/IEC 27004:Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información.
    1. Normas Nacionales de seguridad informática:

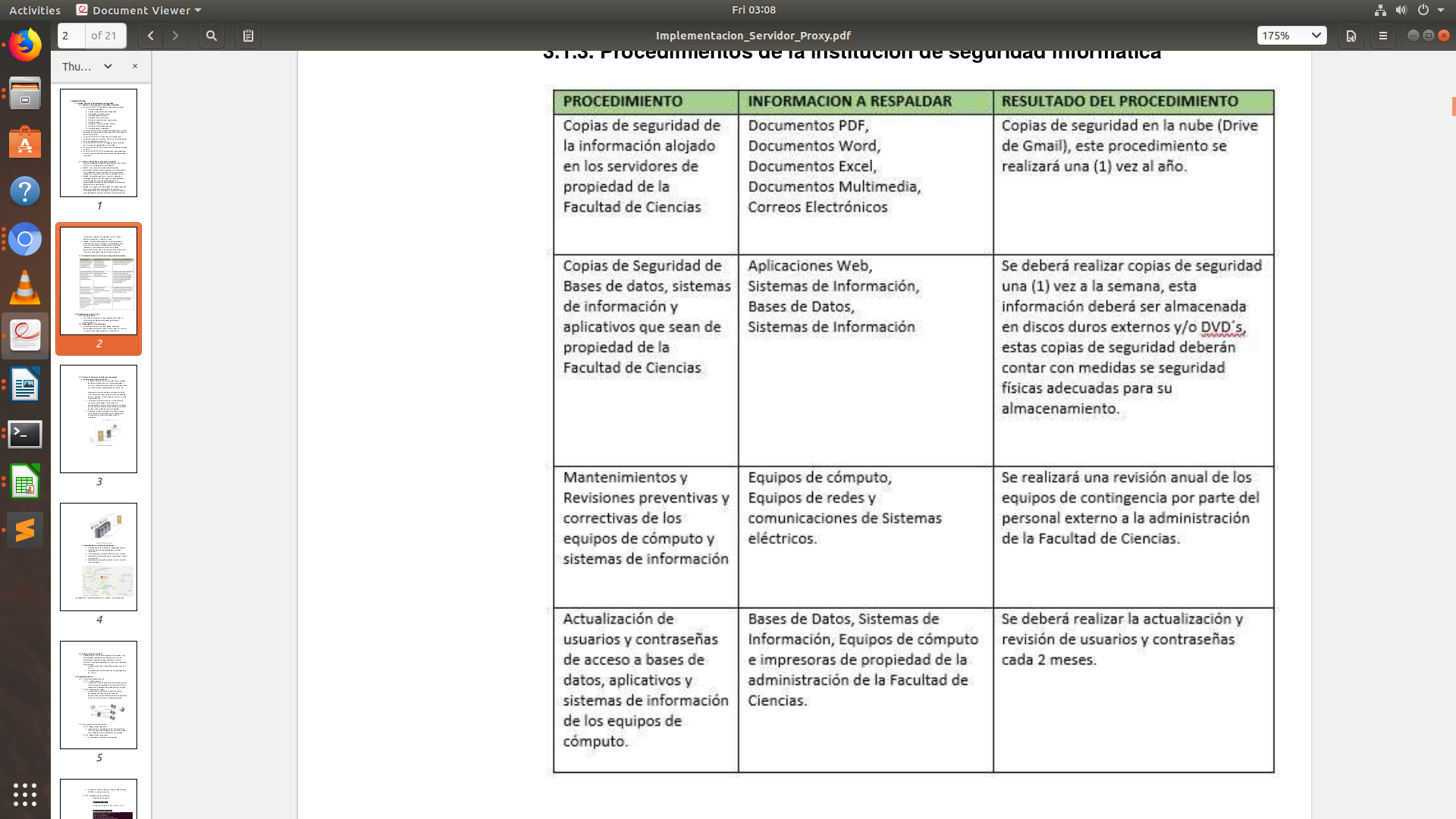
Es de uso obligatorio la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información.

* + - Nota 1: La confianza en el entorno digital o también denominada confianza digital emerge como resultado de cuán veraz, predecible, seguro y confiable son las interacciones digitales que se generan entre empresas, individuos o cosas.
    - Nota 2: Las medidas proactivas y reactivas comprenden tecnología, políticas, controles, programas de capacitación y sensibilización que tienen por finalidad preservar la confidencialidad, integridad y disponibilidad de la información contenida en el entorno digital.
    - Nota 3: Los riesgos en el entorno digital o riesgo de seguridad digital es resultado de una combinación de amenazas y vulnerabilidades en el entorno digital. La gestión del riesgo de seguridad digital comprende los procesos que garantizan que las acciones o medidas son apropiadas con los riesgos y objetivos económicos y sociales en juego.
    - Nota 4: La prosperidad económica y social comprende la creación de riqueza, la innovación, la competitividad, entre otros, así como aspectos vinculados con las libertades individuales, salud, educación, cultura, participación democrática, ciencia, ocio y otras dimensiones del bienestar en las que el entorno digital está impulsando el progreso.
    - DISPOSICIONES COMPLEMENTARIAS:

Medidas de seguridad La Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) promueve permanentemente, en coordinación con las instituciones del sector público, el fortalecimiento de sus medidas de seguridad para la protección de los datos informáticos sensibles y la integridad de sus sistemas informáticos.

Buenas prácticas El Estado peruano realiza acciones conjuntas con otros Estados a fin de poner en marcha acciones y medidas concretas destinadas a combatir el fenómeno de los ataques masivos contra las infraestructuras informáticas y establece los mecanismos de prevención necesarios, incluyendo respuestas coordinadas e intercambio de información y buenas prácticas.

* + 1. Procedimientos de la institución de seguridad informática.



* 1. **Seguridad física y del entorno**

Para garantizar tanto la seguridad del Laboratorio como del hardware presente, se aplican las siguientes medidas:

* + 1. Perímetro físico:

-El Laboratorio de Bioinformática de la UPCH ubicada en la Av.Honorio Delgado 430, San Martin de Porres 15102.

-La seguridad externa de las instalaciones del Laboratorio depende de la UPCH como primer control.

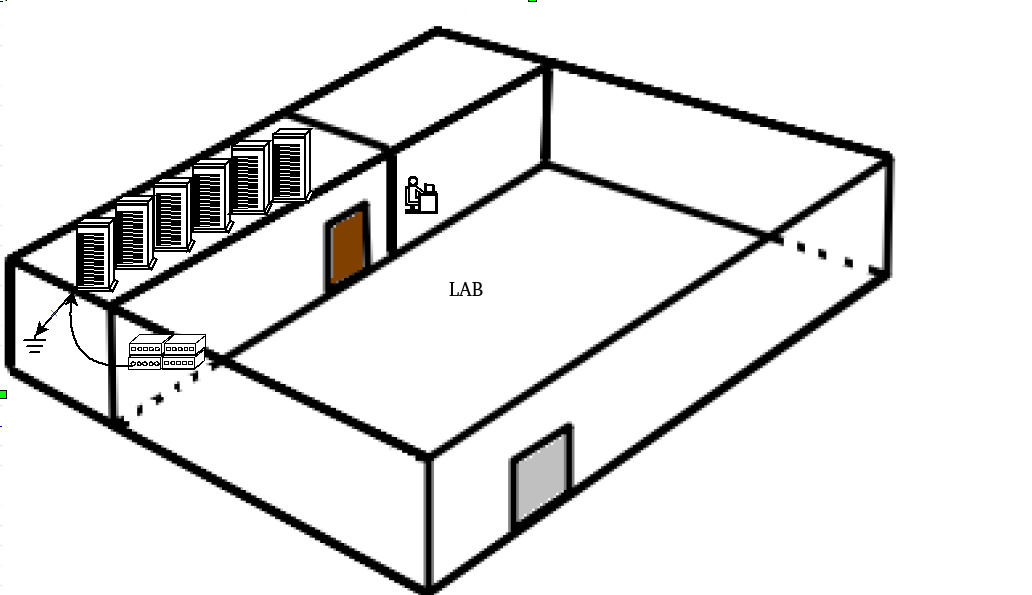
-Cuenta con un adecuado espacio para la distribución de los equipos.

* + 1. Seguridad de la infraestructura:

-Se contara con los respectivos requisitos de funcionamiento de la institución como, presencia de extintores, alarma contra incendios, zonas seguras ante sismos, etc.

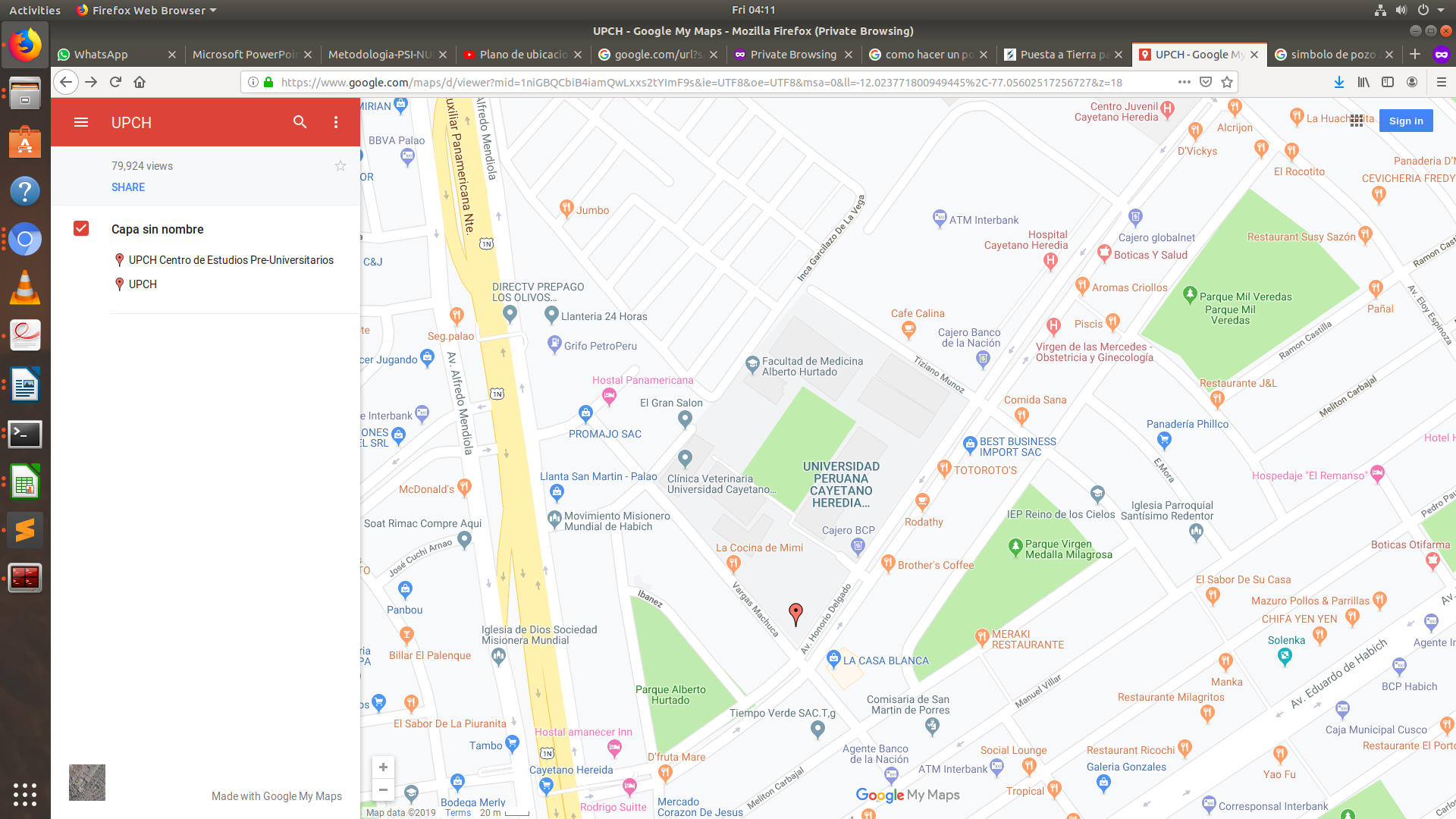
* + 1. Planos de ubicación y distribución de equipos:

El Laboratorio de Bioinformática requiere de un área de oficinas, sala de experimentación e investigación biológica, sala de Cómputo, área de servidores y los servicios higiénicos.



-Luego la sala de Cómputo y el área de servidores.

-Al final estará el área de experimentación e investigación Biológica.



* + 1. Refrigeración del ambiente.- Para mantener un ambiente agradable y preservar los equipos:

-Cada oficina y área, a excepción del área de experimentación, contará con aire acondicionado. Con una temperatura comprendida entre los 18°C y 23°C.

-Las computadoras y servidores contarán con refrigeración líquida.

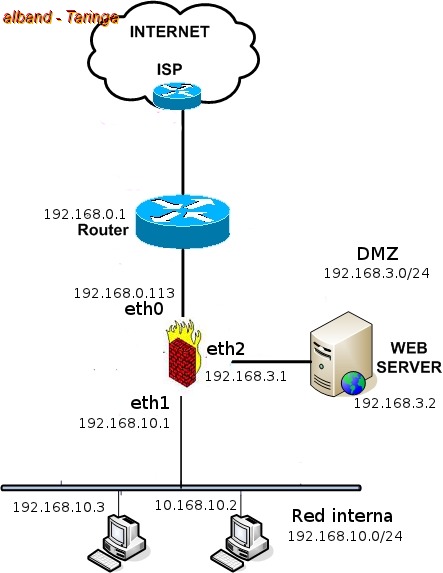
* 1. **Seguridad perimetral**

3.3.1.1 Objetivos:

Proponer un esquema de control de acceso perimetral, tomando en cuenta la seguridad física y lógica de las instalaciones del Laboratorio de Bioinformática.

3.3.1.2 Informe de resultados:

Según los análisis respectivos realizados y descripción de los diferentes niveles de seguridad (seguridad de red, de aplicaciones y de datos), se propone el siguiente diseño:



* + 1. Instalación de sistemas operativos: Para el SO CentOS 7 necesitaremos
       1. Requerimientos generales:

Mínimos: - RAM 1Gb.

- Disco duro 20Gb.

- Frecuencia 1Gz.

Recomendado:- RAM 2 Gb+

- Disco duro 40Gb+

-Frecuencia 1.5Gz+

Es necesario una arquitectura de procesador x86-64.

* + - 1. Requerimientos específicos:

La instalación y configuración se hará en una interfaz gráfica.

Particiones de disco (/boot 400MiB, swap 30GiB y memoria restante /).

Si desea instalarse periféricos adicionales, debe consultarse los drivers de soporte que maneja esta distribución.

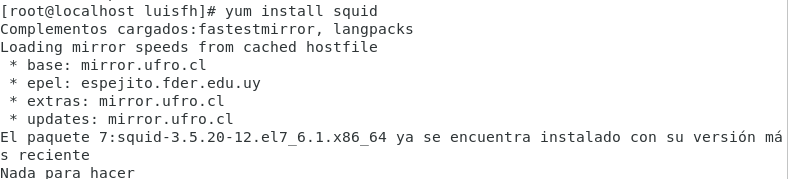
* + - 1. Procedimientos de instalación:

-Abrimos el terminal de CentOS y verificamos la conexión a internet con el comando #ping [www.google.com](http://www.google.com).

-Accedemos como superusuario #su y su respectiva contraseña de root.

-Actualizamos el sistema CentOS 7



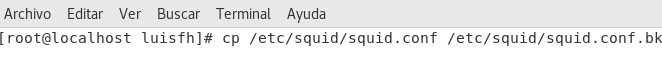
 -Instalamos Squid

* + 1. Configuración de servidor proxy
       1. Requerimientos iniciales:

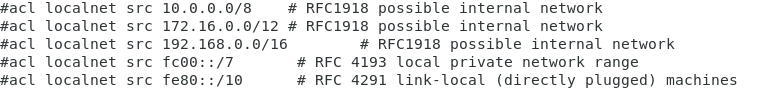
Requerimos paquetes adicionales para la creación de usuarios,

Descargamos el paquete con #yum Install httpd-tools.

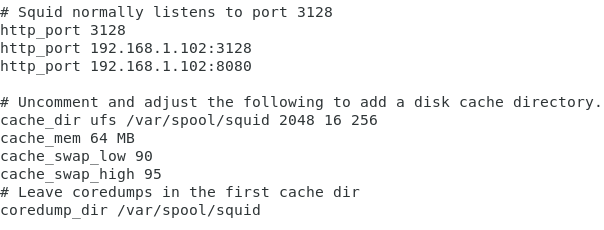
* + - 1. Procedimientos de configuración
         1. Implementación de la solución de proxy:

-Realizamos una copia del archivo Squid.conf.

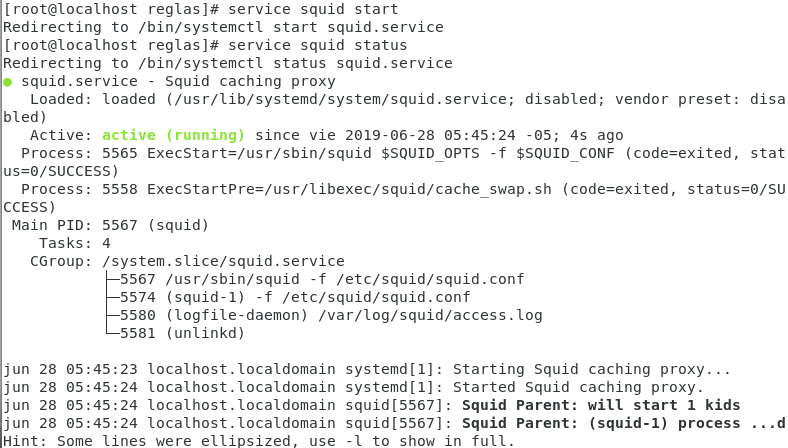
-Accedemos al archivo squid.conf y hacemos las siguientes configuraciones.

-Comentamos las siguientes lineas

-Añadimos los puertos y creamos la cache.



-Guardamos, iniciamos el servicio y verificamos su estatus.



* + - * 1. Implementación de los usuarios y solución filtro de contenidos:

-Creamos la carpeta reglas

-

--Creamos los archivos denegados e ingresamos sus reglas





-Creamos la carpeta patrones e ingresamos sus reglas





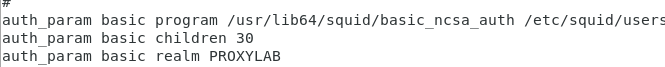
-Creamos la carpeta de usuarios



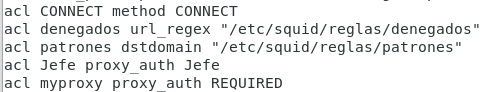
-Creamos los usuarios y sus respectivas contraseñas.



-En el archivo squid.conf, añadimos en la cabecera.

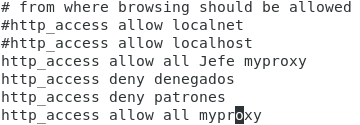


-Creamos las ACL



-

Damos los accesos respectivos.

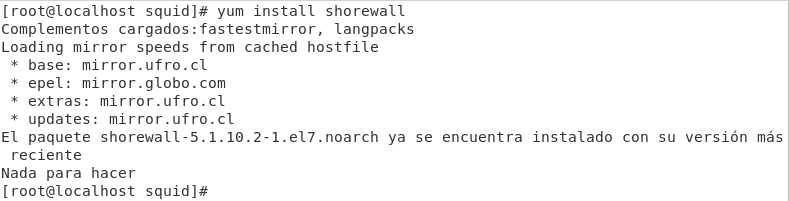


-Reiniciamos el servicio



* + - * 1. Implementación de la solución firewall:

-Implementaremos el firewall Shorewall.

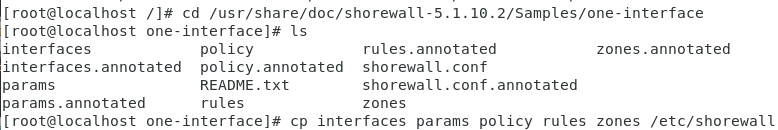


-Accedemos a la carpeta one-interface y copiamos los archivos.

-En la carpeta /etc/shorewall modificamos las copias



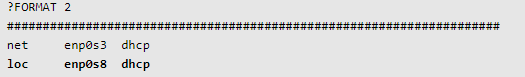
-En el archivo shorewall.conf activamos el shorewall.



-El archivo zones definimos las zonas que administrará el shorewall.



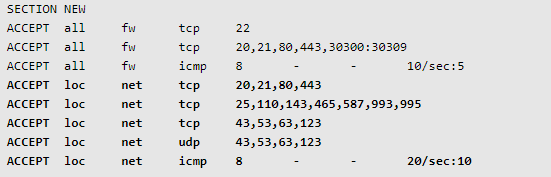
-En el archivo interfaces, la red correspondiente a cada zona



-En el archivo policy, las políticas de acceso



-En el archivo rules definimos las reglas, puertos que se permitirán, entre otras excepciones.



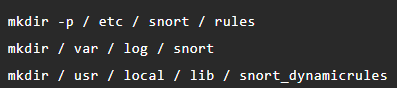
-Iniciamos el servicio



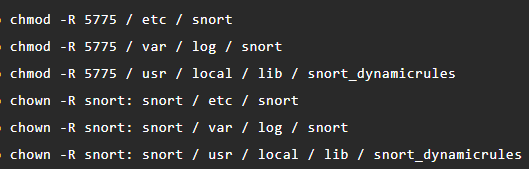
* + - * 1. Implementación de la solución detección de intrusos:

Para ello usaremos el software Snort.

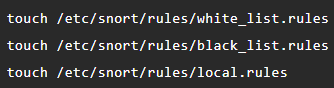
-Instalamos desde el enlace de la página de Snort

-Cr-Creamos las carpetas

-Damos los siguientes permisos



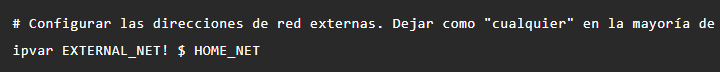
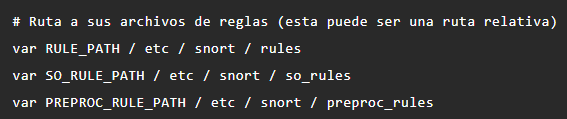
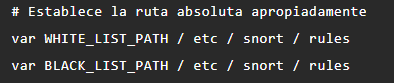
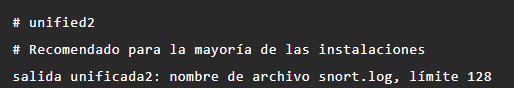
-Creamos las listas blancas, negras y locales

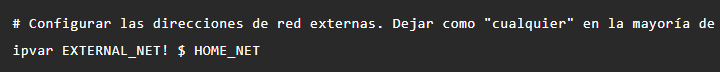


-Descargamos las reglas de la comunidad y las copiamos en la carpeta rules.



-En el archivo snort.conf, modificamos





-Incluimos las re-Incluimos las reglas de detección de intrusos.





-Guardamos y ejecutamos el servicio.



* + - * 1. Implementación de la solución prevención de intrusos:

Implementaremos el programa fail2ban.

-Instalamos fail2ban y los paquetes requeridos para trabajar con shorewall





-Creamos el archivo jail.local.

-Agregamos el tiempo que será baneado un externo

-El tiempo de búsqueda en el cual será baneado.

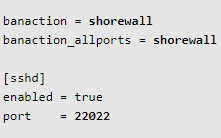
-El máximo de intentos para ser baneado.

-El rango de ips ignoradas.



-fail2ban emplea iptables como medio de bloqueo por defecto, pero estamos usando shorewall quien tomara las acciones de baneo.

- Habilitamos el puerto para las Conexiones SSH.



-Iniciamos el servicio



* + - * 1. Implementación de la solución controlador ancho de banda

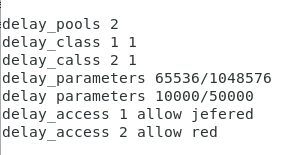
Esto lo logramos con nuestro programa Squid.

-Para ello restringiremos el ancho de banda a toda la red en 10Kb, menos al jefe que tendrá un ancho de 65Kb.

-En el archivo Squid.conf, añadimos las acls



-Limitamos los anchos de banda.



* 1. **Seguridad de red propiamente dicha**

Si una persona no autorizada posee acceso a la red interna del laboratorio de bioinformática, potencialmente puede acceder a cualquier puerto de cualquier equipo o monitorizar el tráfico que circula por la red, de forma pasiva (solo de lectura) o activa (modificable). Para proteger la rede de estas amenazas se puede utilizar sistemas de detección de intruso, segmentación de redes mediante routers y switches, utilizando IPSEC y/o SSL para cifrado durante el transporte de datos

* + 1. Ubicación y protección de los equipos

Los equipos que utilizaremos para la implementación de la seguridad perimetral serán dentro del cuarto de servidores donde este estará con un acceso restringido a personas solo con el acceso a esa parte del laboratorio y con un mejor ambiente para el funcionamiento de nuestro equipo.

* + 1. Suministro de energía

La empresa Luz del Sur proporciona la energía a la institución; Cuenta con un estabilizador de 8 conexiones de 3 puntos de muy buena calidad que convierte la corriente alterna a una corriente continua muy estable y todo está conectado a un generador de respaldo que en caso de falla del suministro eléctrico.

* + 1. Suministro del cableado

El cableado de nuestros equipos se encuentra de manera que interfiera en el flujo del personal con acceso al cuarto de servidores y en la parte alta del cuarto de servidores.

* + 1. Mantenimiento de equipos

Nuestro equipo al ser parte clave de la seguridad de protección de información del laboratorio esta contará con un mantenimiento trimestral periódico al igual que los servidores que se encuentran en el cuarto de servidores.

* + 1. Proteger de vulnerabilidades de seguridad

Usando Squid protegemos al laboratorio de vulnerabilidades no obstante no todo sistema de seguridad es ideal por lo que estaremos actualizando las configuraciones del Squid y actualizar los permisos a accesos y restricciones de nuestra seguridad perimetral.

* + 1. Acceso restringido a la red

Estamos estableciendo un acceso restringido a la red del laboratorio usando la ayuda del Squid para evitar que una persona no autorizada que no tenga el acceso a la red laboratorio.

* 1. **Seguridad de equipos**
* La seguridad de equipos tanto servidores como clientes implica las siguientes tareas: mantenerse al día con los parches de seguridad, desactivar todos los servicios innecesarios y mantener el Squid activo y constantemente actualizado. El mayor riesgo es cuando el atacante puede acceder al equipo a través de vulnerabilidades a la red del laboratorio.
  + 1. Distribución adecuada de equipos

Los equipos se encuentran bien espaciados con los servidores y PC’s del cuarto de servidores de manera que, si ocurre algún incidente con nuestros equipos, estos no se afecten entre sí.

* + 1. Pozo de tierra

Todos los elementos de nuestro equipo están conectado a un estabilizador de 3 polos de los cuales uno es conexión a tierra en casos de falla del estabilizador nuestros equipos no se dañarán.

Hay además 2 hilos conectores a tierra que garantizan una mayor seguridad para todo el laboratorio.





Corei9 9900k

Gtx1080ti

64 ram

* + 1. Instalaciones y configuración adecuada

La aplicación de Squid está configurada dentro del sistema operativo CentOS donde fortalecemos las vulnerabilidades tanto de la red interna como del sistema operativo.

* 1. **Seguridad de aplicaciones**
     1. Uso restringido de aplicativos

Las aplicaciones se protegen realizando un control de acceso mediante la sólida implantación de mecanismos de autentificación y autorización.

* + 1. Navegación web restringida

A través del firewall restringiremos el tráfico específico de las aplicaciones a correos (SMTP), web (http) entre otras.

* 1. **Seguridad de datos**

Si un atacante ha traspasado todas las barreras anteriores y posee acceso a la aplicación, autentificación y autorización, así como el cifrado, constituyen las tecnologías más empleadas para proteger los datos.

* + 1. Sistema de backup

Para el caso expuesto previamente necesitamos un respaldo de la data del laboratorio en los discos duros de respaldos que tenemos.

* + 1. Acceso restringido a la información

Con la seguridad perimetral implementada priorizamos cuidar que no se violen la Autenticidad, Integridad, Disponibilidad, Confidencialidad

**4. PRUEBAS**

**4.1. Prueba de Usabilidad**

**-**Servicio de proxy activo

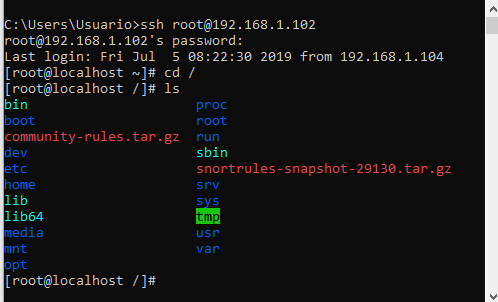
**-**Ingreso de usuario

**-**Bloqueo de páginas



-Servicio Shorewall

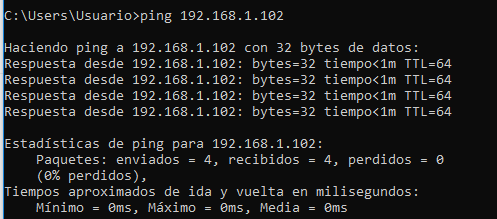
-Puerto SSH permitido



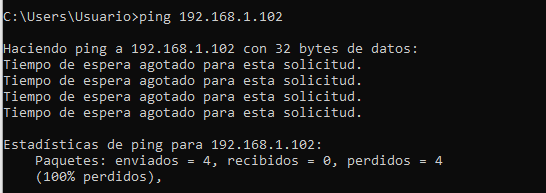
**4.4. Prueba de Seguridad y Controles**

-Servicio shorewall

-Reconoce el host

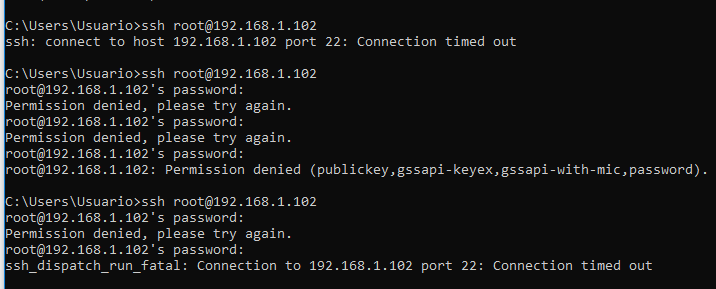


-Bloquea el tráfico

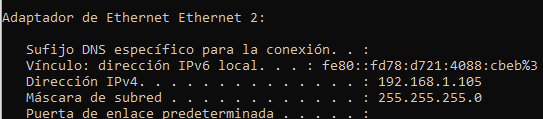


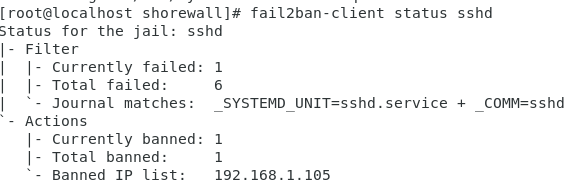
-Servicio Fail2ban

-Solicitando conexión por el puerto ssh, 5 intentos fallidos adrede.



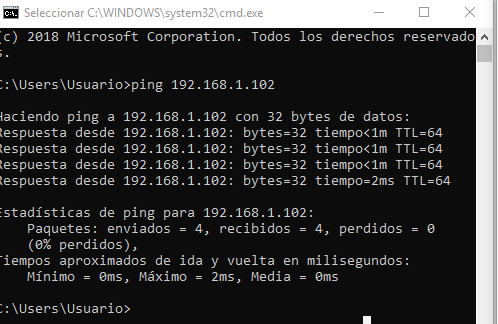
-Bloqueo de la ip



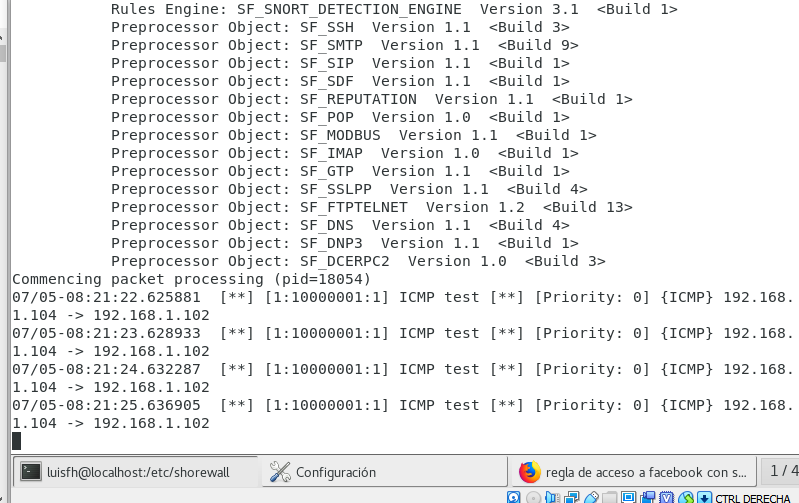


-Servicio Snort

-Ping no permitido



-Aviso de alerta



**5. CONCLUSION Y RECOMENDACIONES**

**5.1. Conclusión**

**-**El servidor proxy mejora el rendimiento de la red como los accesos a ella, regula el ancho de banda.

**-**Filtrado de contenidos eficientemente, necesario para la eficiencia de los trabajadores evitando posibles distracciones.

-El trabajo en conjunto del Servidor proxy, Shorewall, Fail2ban y Snort, mejoran la seguridad de la red, de los usuarios y la información.

**5.2. Recomendaciones**

**-**Realizar un testeo periódico del sistema.

**-**Ante el constante avance del cybercrimen, actualizar los componentes del software periódicamente.

**6. BIBLIOGRAFIA**

* Informe de tesis en la Pontificia Universidad Católica del Perú: Diseño de una arquitectura de seguridad perimetral de una red de computadoras para una empresa pequeña.

Autor: Valenzuela Gonzales, Jorge Luis. Lima-Perú

* Informe de Tesis en la ESPE: Implementación de un sistema de seguridad perimetral para las empresas Teamsourcing Cía. Ltda. Con software libre (ClearOS) y desarrollo de las políticas de seguridad basadas en el estándar ISO-27001.
* Informe de Tesis en la Universidad Nacional de Trujillo: Diseño de un modelo de red de zona perimetral segura para PYMES del Valle Jequetepeque.

Autor: Sánchez Quiroz, Bertha Natalí. Trujillo-Perú.