ACTA DE REUNIÓN		
Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia (CTIC-EPB)		
Grupo de Trabajo: SEGURIDAD		
Correlativo: CTIC-SE-04/2019	**Fecha: 02-05-2019**	**Página:** 1/5
Elaborado por: Andre Mitsutake Cueto		

ASISTENTES:

De acuerdo a la lista adjunta.

AGENDA DE TRABAJO:

1. Revisión y comentarios la designación de puntos a desarrollar (Tabla IP privadas,Abreviaciones).
2. Revisión y comentarios de propuestas de seguridad sobre Modelo OSI (Capa de Transporte).
3. Análisis de propuestas de seguridad sobre Modelo OSI (Capa de Transporte).
4. Aprobación de redacciones.
5. Designación de puntos para desarrollar.
6. Acuerdos para la siguiente reunión.

DESARROLLO:

- Tabla para Jerarquizar la asignación de redes IP privadas (ANEXOS) – Aprobado

RFC 1918: La Autoridad de Números Asignados de Internet (IANA), ha reservado los siguientes tres bloques de espacio de direcciones IP para redes privadas.

CLASE	IP [RANGO]	PREFIJO	# HOSTS	USO
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8	16777214	Red Perimetral
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12	1048574	Red Core (DMZ)
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16	65534	Red de Acceso

- Glosario, abreviaciones técnicas (Sergio Rojas)

Glosario

Li-Fi.- Deriva del latín y es una abreviatura de Fidelidad a la Luz, el Li-Fi es una tecnología utilizada para la comunicación inalámbrica entre dispositivos, ésta comunicación se da gracias a la luz que es utilizada para transmitir tanto datos como referencias de posición. En su estado actual de desarrollo, solamente es posible la utilización de lámparas LED las cuales permiten la transmisión de luz visible.

En términos técnicos, Li-Fi es un sistema de comunicaciones con luz visible que es capaz de transmitir datos a altas velocidades a través del espectro de luz visible, radiación ultravioleta e infrarroja.

En términos de su uso final, la tecnología es similar a la del Wi-Fi. La diferencia técnica clave para distinguir estas dos tecnologías es que el Wi-Fi utiliza una frecuencia de radio para transmitir datos. En cambio el Li-Fi, hace uso de la luz para transmitir datos, motivo por el cual el Li-Fi ofrezca distintas ventajas, como por ejemplo el poder trabajar a través de un ancho de banda más alto, o trabajar en áreas susceptibles a interferencias

electromagnéticas (cabinas de aviones, hospitales) además ofrecer velocidades de transmisión más altas. La tecnología está siendo en la actualidad desarrollada activamente por varias organizaciones en todo el mundo.

Direcciones MAC.- Una dirección MAC es el identificador único asignado por el fabricante a una pieza de hardware de red (como una tarjeta inalámbrica o una tarjeta Ethernet). «MAC» significa Media Access Control, y cada código tiene la intención de ser único para un dispositivo en particular.

Una dirección MAC consiste en seis grupos de dos caracteres, cada uno de ellos separado por dos puntos. 00:1B:44:11:3A:B7 es un ejemplo de dirección MAC.

Estructura de Switch.- Switch case es una estructura de control empleada en programación. Se utiliza para agilizar la toma de decisiones múltiples; trabaja de la misma manera que lo harían sucesivos if, if else o until anidados, así como combinaciones propias de determinados lenguajes de programación.

El switch no es tan popular como el if, pero se utiliza con regularidad en la programación. En principio la funcionalidad de un switch también se puede implementar con múltiples if anidados. En el caso de que haya muchas acciones dependientes de muchos valores iniciales, es recomendable su uso. El switch favorece la Facilidad y rapidez en la programación.

El switch no solo te ayuda en ciertos casos. Si no que te permite realizar " Opciones " Que en un if no lo pudieras hacer".

Patch Panel.- Se trata de un panel de conexión, un compartimento de conexión, un campo de conexión o un campo de conexión es un dispositivo o unidad con una serie de conexiones, generalmente del mismo tipo o similar, para el uso de circuitos de conexión y enrutamiento para monitorear, interconectar y probar circuitos de manera conveniente. , de manera flexible. Los paneles de conexión se usan comúnmente en redes de computadoras, estudios de grabación, radio y televisión.

El término "parche" provino del uso temprano en estudios de radio y telefonía, donde el equipo adicional que se mantiene en modo de espera podría ser sustituido temporalmente por dispositivos fallidos. Esta reconexión se realizó a través de cables de conexión y paneles de conexión, como los campos de conexión de las centrales telefónicas tipo cable.

Conexiones de Redundancia.- Los sistemas redundantes o conexiones de Redundancia, en ingeniería de computadores, son aquellos en los que se repiten aquellos datos o hardware de carácter crítico que se quiere asegurar ante los posibles fallos que puedan surgir por su uso continuado.

Se presenta como una solución a los problemas de protección y confiabilidad. Este tipo de sistemas se encarga de realizar el mismo proceso en más de una estación, ya que si por algún motivo alguna dejara de

funcionar o colapsara, inmediatamente otro tendría que ocupar su lugar y realizar las tareas del anterior.

Las técnicas de redundancia han sido usadas por la industria militar y aerospacial por muchos años para alcanzar una alta confiabilidad. Una base de datos replicada es un ejemplo de sistema distribuido redundante.

Network Address Traslation.- La traducción de direcciones de red (NAT) es un método para volver a asignar un espacio de direcciones IP a otro modificando la información de la dirección de red en el encabezado IP de los paquetes mientras están en tránsito a través de un dispositivo de enrutamiento de tráfico. La técnica se usó originalmente como acceso directo para evitar la necesidad de redireccionar cada host cuando se movía una red. Se ha convertido en una herramienta popular y esencial para conservar el espacio de direcciones global frente al agotamiento de direcciones IPv4. Se puede usar una dirección IP enrutable de Internet de una puerta de enlace NAT para una red privada completa.

El enmascaramiento de IP es una técnica que oculta un espacio completo de direcciones IP, que generalmente consiste en direcciones IP privadas, detrás de una dirección IP única en otro espacio de direcciones, generalmente público. Las direcciones ocultas se cambian a una única dirección IP (pública) como la dirección de origen de los paquetes IP salientes, por lo que aparecen como originadas no desde el host oculto sino desde el propio dispositivo de enrutamiento. Debido a la popularidad de esta técnica para conservar el espacio de direcciones IPv4, el término NAT se ha convertido prácticamente en sinónimo de enmascaramiento de IP.

Como la traducción de la dirección de red modifica la información de la dirección IP en paquetes, tiene serias consecuencias en la calidad de la conectividad a Internet y requiere una cuidadosa atención a los detalles de su implementación. Las implementaciones de NAT varían ampliamente en su comportamiento específico en varios casos de direccionamiento y su efecto en el tráfico de red. Los proveedores de equipos que contienen implementaciones de NAT no documentan los aspectos específicos del comportamiento de NAT.

Una Lista de Control de Acceso o ACL (del inglés, Access Control List) es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

Las ACLs permiten controlar el flujo del tráfico en equipos de redes, tales como routers y switches. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición. Sin embargo, también tienen usos adicionales, como por ejemplo, distinguir “tráfico interesante” (tráfico suficientemente importante como para activar o mantener una conexión) en ISDN.

En redes de computadoras, ACL se refiere a una lista de reglas que detallan puertos de servicio o nombres de dominios (de redes) que están disponibles en una terminal u otro dispositivo de capa de red, cada uno de ellos con una lista de terminales y/o redes que tienen permiso para usar el servicio. Tantos servidores individuales como routers pueden tener ACLs de redes. Las listas de acceso de control pueden configurarse generalmente

ACTA DE REUNIÓN		
Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia (CTIC-EPB)		
Grupo de Trabajo: SEGURIDAD		
Correlativo: CTIC-SE-04/2019	**Fecha: 02-05-2019**	**Página:** 4/5
Elaborado por: Andre Mitsutake Cueto		

para controlar tráfico entrante y saliente y en este contexto son similares a unos cortafuegos.

Existen dos tipos de ACL:
- ACL estándar, donde solo tenemos que especificar una dirección de origen;
- ACL extendida, en cuya sintaxis aparece el protocolo y una dirección de origen y de destino.

Capa enlace de Datos - Aprobado
Lineamiento:
- Se debe usar protocolos de seguridad autenticación en redes inalámbricas no vulnerables (WPA2 y WPA3).

Buena Practica:
- Se recomienda emplear el uso de Firewall para redes inalámbricas a partir de la infraestructura corporativa.

3. Capa IP - Aprobado
- Se debe implementar ACL para la administración de dispositivos de comunicación

4. Capa de transporte - Aprobado
Lineamiento:
- Se debe aplicar los protocolos de comunicación que utilicen cifrado integrado (Anexo – Protocolos mas usados).
- Se debe implementar ACL-extendidas para tener mayor control de los servicios y segmentos críticos.
- Se debe habilitar únicamente los puertos de los servicios utilizados por la institución (ingress-filtering).

8. Diseño de red
Requisitos mínimos de infraestructura de redes
- Dispositivo de protección perimetral
- Uso de Switch’s en vez de HUB’s

Se debe implementar un servicio local NTP – IBMetro.
Se debe Infraestructura (Revisar – Andre).
Se debe tener la siguiente documentación de red mínima:
- Lógica
- Física
- Diagramas Horizontales y Verticales
- Inventario de segmentos de red
- Inventario de equipos de red

Se debe tener una bitácora de cambios de configuración en equipos de red de la institución (PISI – Andre).

ACTA DE REUNIÓN		
Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia (CTIC-EPB)		
Grupo de Trabajo: SEGURIDAD		
Correlativo: CTIC-SE-04/2019	**Fecha: 02-05-2019**	**Página:** 5/5
Elaborado por: Andre Mitsutake Cueto		

Referencias Lineamientos:

- Se recomienda la implementación de syslog-server.
- Se recomienda mantener actualizado el fimware de los equipos de comunicación de la institución.
- Se recomienda la implementación de IDS-IPS.

DESIGNACIÓN DE PUNTOS A DESARROLLAR:

- Revisión de Glosario, análisis de definiciones y redacciones => TODOS
- Tabla de protocolos mas usados => Dennis BCB

ACUERDOS Y COMPROMISOS:

Sugerencias en la Capa Diseño de red [Lineamientos y Buenas Practicas]=> TODOS
Referencias de otros lineamientos => ANDRE