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-07/2019	**Fecha: 03-06-2019**	**Página:** 1/14
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 (Dispositivos de Redes).
2. Revisión y comentarios de propuestas relacionados a otros lineamientos (lineamientos y buenas practicas)
3. Análisis de propuestas y observaciones.
4. Aprobación de redacciones.
5. Designación de puntos para desarrollar.
6. Acuerdos para la siguiente reunión.

DESARROLLO:

5. Términos y definiciones

Entidad del sector público: Entidades públicas del nivel central del Estado; instituciones descentralizadas, autónomas, estratégicas, empresas públicas; empresas estatales mixtas; empresas estatales intergubernamentales y otras entidades públicas no incluidas en las categorías señaladas precedentemente.

- **Integridad:** Propiedad que salvaguarda la exactitud y completitud de la información.
- **Disponibilidad:** Propiedad de acceso y uso de información a entidades autorizadas cuando estas lo requieran.
- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **No Repudio:** Según [CCN-STIC-405:2006]: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación.
  Según [OSI ISO-7498-2]: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).
- **Redes:** conjunto de equipos (computadoras, periféricos, etc.) que están interconectados y que comparten diversos recursos.
- **Plan de Contingencia:** Es un instrumento que comprende métodos y el conjunto de acciones para el

buen gobierno de las Tecnologías de la Información y Comunicación en el dominio del soporte y el desempeño, contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del servicio y las operaciones de una entidad, en circunstancias de riesgo, crisis y otras situaciones anómalas.

- **Responsable de Seguridad de la Información (RSI):** Servidor público responsable de gestionar, planificar, desarrollar e implementar el Plan Institucional de Seguridad de la Información.

- **Seguridad de la Información:** La seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad.

- **Seguridad Informática:** Es el conjunto de normas, procedimientos y herramientas que se enfocan en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante.

- **Li-Fi:** Tecnología utilizada para la comunicación inalámbrica entre dispositivos capaz de transmitir datos a altas velocidad a través del espectro de luz visible.

- **MAC:** Media Access Control-MAC, identificador único asignado por el fabricante a una pieza de hardware de red (como una tarjeta inalámbrica o una tarjeta Ethernet).

- **NAT:** Network Address Traslation-NAT, 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.

- **ACL:** Access Control List-ACL, concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.
    - ACL (estándar), donde solo tenemos que especificar una direcciones IP's.
    - ACL (extendida), en cuya sintaxis aparece el protocolo y dirección IP's.

6. Lineamientos y buenas practicas

Todos los servicios telemáticos de las entidades publicas se constituye en un componente de vital importancia en las operaciones y funciones de la institución. Por tanto, el establecimiento de lineamientos y buenas practicas para su implementación es igualmente fundamental.

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-07/2019	**Fecha: 03-06-2019**	**Página:** 3/14
Elaborado por: Andre Mitsutake Cueto		

Los lineamientos enmarcados en este documento establecen estándares técnicos mínimos requeridos, a ser implementados o adecuados para la mejora de seguridad en la infraestructura de redes en todas las entidades del sector publico del Estado Plurinacional de Bolivia. Las buenas practicas consisten en recomendaciones (opcionales) para la mejora de seguridad.

Los lineamientos técnicos y buenas practicas se establecen para los siguientes elementos o subsistemas que componen una infraestructura de redes:

- Diseño e implementación de Seguridad en Redes.
- Seguridad de red perimetral.
- Seguridad en accesos remotos.
- Seguridad en redes Inalámbricas.
- Gestión y monitoreo de redes.
- Seguridad MAN/WAN.
- Seguridad de servicios/aplicaciones.

A continuación se desarrolla cada uno de ellos:

6.1]Diseño e implementación de Seguridad en Redes
6.1.1 Infraestructura de Seguridad de Red
Los lineamientos y buenas practicas descritos en al infraestructura de seguridad de redes están compuestas por las instalaciones de la red de transmisión y partes de redes individuales que están protegidas con mecanismos de implementados en la dimensiones de seguridad. Algunos ejemplos de los componentes que pertenecen a la capa de seguridad en infraestructura son enrutadores, conmutadores, cortafuegos, etc. A seguir los lineamientos necesarios:

- Se debe constar con dispositivo de protección perimetral, cortafuegos, para el bloqueo de accesos no autorizados y al mismo tiempo permitiendo comunicaciones autorizadas hacia la institución.

- Se debe usar dispositivos Switch (conmutador) en vez HUB (concentrador) a nivel de acceso de cada institución.

- Se debe usar dispositivo de capa 3 (switch-capa3, enrutador, etc.), para la administracion de subredes de la institución.

- Se debe implementar servicio local NTP – IBMetro ó GMT-4, con el fin de que todos los equipos conciban los tiempos de la misma manera.

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-07/2019	**Fecha: 03-06-2019**	**Página:** 4/14
Elaborado por: Andre Mitsutake Cueto		

- Se debe realizar la securización (Hardening) de todo dispositivos implementado en la red de la institución (Anexo).

El siguiente lineamiento tiene como referencia "*Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público*".

- *Considerar la implementación de dispositivos de red redundantes para puntos de fallo único donde la disponibilidad sea un factor crítico.*

Los puntos a mencionar se encuentra plasmados en el "*Lineamiento y buenas practicas para la implementación de un Centro de Procesamientos de Datos",* los cuales serán de carácter obligatorio en la implementación de infraestructura de seguridad de redes.

- *Identificar y etiquetar de manera apropiada todo el equipamiento, medios de distribución y accesorios empleados en la implementación.*

Como buenas practicas para la implementación de infraestructura de seguridad de redes se puede recomendar:

- La implementación de Proxy-Firewall (programa o dispositivo), para proteger y mejorar el acceso a servicios web.
- La implementación de Cortafuegos-UTM (Unified Thread Management) para pequeñas y medianas instituciones.
- La implementación de Cortafuegos-NGFW (Next Generation Firewall) para grandes instituciones.
- La implementación de Sistemas de Detección de Intrusos (IDS) y/o Sistemas de Prevención de Intrusos (IPS) en la institución correspondiente.
- La implementación de sistemas WAF, para la inspección de trafico HTTP, protegiendo así ataques tales como Inyección SQL, XSS, CSRF, etc.
- La implementación de sistema de Filtrado de Contenido, para el filtrado de contenido que puede tener acceso los usuarios de la institución. Este filtrado puede estar relacionado a pagina web, e-mail, etc.
- La implementación de sistemas de Gestión de Información y Eventos de Seguridad (SIEM), para la detección de posibles amenazas informáticas y su rápida resolución.
- La implementación de Honeypot, para engañar a los posibles cibercriminales, y de esta manera contener ataques peligrosos y analizar los movimientos de los cibercriminales para futuros ataques.
- La implementación de mecanismos de seguridad tales como el SanBox, para disponer de un entorno aislado sin comprometer el resto de la infraestructura, de programas maliciosos.
- La implementación de soluciones Anti-SPAM para la mitigacion de amenazas tales como phising, spam y amenazas zombies-originadas.

- La implementación de dispositivos para salvaguardar la seguridad telematica siempre y cuando estas sean requeridas por los servicios y operaciones que cumple la institución

6.1.2 LAN alambrada

Nodos conectados en una red a través de un dispositivo de red utilizando cables de red, los cuales transfiere datos a altas velocidades. A continuación se presenta lineamientos para la implementación de una red alambrada LAN, la cual se encuentra plasmada en los "*Lineamientos y buenas prácticas para la implementación de un Centro de Procesamiento de Datos*".

- *Debe estar listo para permitir un crecimiento del 40% en el cableado de datos.*
- *En caso de utilizar cables de cobre, estos deben cumplir con la norma ANSI/TIA/EIA-568-B.2-10 o normas vigentes.*
- *En caso de utilizar cables de fibra óptica, estos deben cumplir con la norma ANSI/TIA/EIA-568-B.3 o normas vigentes.*
- *Identificar y/o etiquetar de forma apropiada todo el cableado entre los diferentes niveles, según la nomenclatura adoptada por la institución.*

Las buenas practicas para la red LAN alambrada recomiendan:

- Emplear estándares de IEEE 802.3 para la implementación de medios físicos de comunicación.
- Tener conexiones de redundancia en comunicaciones críticas dentro de la red local de la entidad.
- Reducir al mínimo los puntos únicos de falla de la infraestructura de red.
- Uso de la tecnología más eficiente para la implementación en la infraestructura de red local de la institución, fibra óptica, cables coaxiales o cables de par trenzado.

- Toda terminal cliente (roseta de conexión) esté debidamente protegida del acceso sin vigilancia y en caso de estar en estado pasivo (No activo), su terminal del lado de la distribución (Patchpanel) está desconectada del arreglo de switchs hasta que la misma sea requerida; asegurando que no sea un punto de acceso sin control o un punto susceptible a vulneración (Medios de protección de puertos en el switch).

A seguir se menciona buenas practicas, plasmadas en el "*Lineamientos y buenas prácticas para la implementación de un Centro de Procesamiento de Datos*".

- *A lo largo de todo el trayecto del cableado no se deben permitir puentes, derivaciones y empalmes.*
- *Respetar la longitud máxima establecida del tendido de cableado estructurado de datos de acuerdo a la tecnología utilizada.(Anexo)*

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-07/2019	**Fecha: 03-06-2019**	**Página:** 6/14
Elaborado por: Andre Mitsutake Cueto		

- *Todo el cableado de conexión de equipos terminales debe estar apropiadamente identificado y/o etiquetado, según la nomenclatura adoptada por la institución.*
- *No se deben permitir puentes, derivaciones y empalmes a lo largo de todo el trayecto del cableado, entre estaciones de distribución o repetición.*
- *La capacidad de transmisión de datos deberá ser mayor al consumo máximo planificado del cableado horizontal.*
- *Se debe elaborar la documentación referida al manual de operación y hojas de datos de las estaciones de distribución o repetición instaladas.*
- *El sistema de escalerillas deberá organizar el cableado de datos y energía de manera separada para evitar el cruce o superposición de los mismos.*
- *Asegurar debidamente los cables dentro del sistema de escalerillas.*
- *El sistema de escalerillas debe ser de un material inoxidable.*
- *El cableado estructurado instalado en el CPD se ajuste a los diversos estándares que existen: norma americana (TIA, BICSI), norma europea (EN) y normas internacionales (ISO/IEC). Cada institución debe elegir y aplicar el estándar que se adecúe mejor a sus necesidades y objetivos.*
- *Mantener una distancia apropiada mínima de 15 cm. entre el cableado estructurado de datos con el cableado eléctrico para evitar interferencia electromagnética.*
- *Los ductos de cableado estructurado deben estar destinados exclusivamente para ese fin y estar correctamente dimensionados, para evitar saturación de cables.*
- *Los ductos de paso de cables entre pisos y paredes no deben estar obstruidos ni presentar saturación de cables y deben tener medios de agrupación de cables apropiados.*
- *El cableado vertical debe realizar su recorrido por un shaft independiente.*
- *En caso de utilizar cables de cobre y/o fibra óptica, la cobertura debe tener la característica de emisión de baja cantidad de humo ante la exposición al fuego y estar hecha de material que no contenga sustancias halógenas para reducir la cantidad de gases tóxicos y corrosivos emitidos durante su combustión (IEC 60332).*
- *Si se utilizan patch cords de cobre y/o fibra óptica, estos deben estar preconectorizados y certificados de fábrica.*
- *En caso de utilizar patch panels de cobre, estos deben ser modulares de uno (1) o dos (2) RU (unidades de rack) con espacios para colocar jacks de datos.*
- *En caso de utilizar bandejas de fibra óptica, estas deben estar preparadas para el uso de casetes, cordones y cables pre-conectorizados.*
- *En caso de utilizar bandejas de fibra óptica, estas deben ser corredizas, tener tapa y ordenadores interiores para proteger las conexiones de fibra óptica instaladas provenientes de las acometidas.*
- *Instalar ordenadores de cables que faciliten el debido agrupamiento de la densidad de patch cords.*

6.1.3 Control de acceso a red cableada (Control de acceso a la red)

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-07/2019	**Fecha: 03-06-2019**	**Página:** 7/14
Elaborado por: Andre Mitsutake Cueto		

El enfoque del control de acceso a red se basa en implementar controles de acceso en la institución para evitar el acceso no autorizando de usuarios. Los siguientes puntos reflejan los lineamientos para el control de acceso a red cableada:

- Se debe tener registro e implementación de control de todas las direcciones MAC de los equipos que pertenecen a la entidad pública para el control y autorización en el acceso a la red local.
- Se debe tener registro e implementación de control de todas las direcciones MAC de los equipos pertenecientes a los servidores públicos autorizados para el acceso a la red local.
- El registro de direcciones MAC de equipos invitados no será obligatorio, pero los mismos deberán tener acceso restringido a la red local.

Como buenas practicas considerando la cantidad de usuarios y equipos relacionados a la infraestructura de redes, se recomienda:

- Implementar el protocolo 802.1x conforme a la cantidad de registros de direcciones MAC de la entidad.
- Implementar Spanning Tree - STP cuando se tenga una estructura de red local amplia.
- Limitar el uso de las redes troncales VLAN’s de la red local de la entidad.

6.1.4 Direccionamiento / Segmentación de Red

La necesidad de usar direcciones IP que se ajuste al crecimiento y control de los dispositivos de redes. La segmentación de red o "zonificación" puede proporcionar un control eficaz de mitigar el siguiente paso de una intrusión en la red y para limitar aún más el movimiento a través de la red o propagación de una amenaza. De esta manera se está minimizando esencialmente el nivel de acceso a la información sensible para las aplicaciones, los servidores y las personas que no lo necesitan, al tiempo que permite el acceso de los que lo hacen. Para este propósito, se deben seguir los siguientes lineamientos:

- Se debe hacer un relacionamiento entre direcciones IP, MAC Address y otros campos descriptivos.
- Se debe usar un rango de IP’s estáticos en la publicación de servicios institucionales, para su delimitación.
- Se debe implementar Listas de Control de Accesos (Access Control List - ACL) para segmentos críticos en la infraestructura de la red institucional. (agregar glosario de terminologías)
- Se debe implementar Listas de Control de Accesos (Access Control List - ACL) para la administración de dispositivos de comunicación.
- Se debe segmentar las redes independientes, usar CIDR (Class Inter Domain Routing) de acuerdo a la necesidad, separando por áreas y/o servicios tales (administración, recursos humanos, VoIP, etc.)

Tomando referencia del “*Lineamientos para la elaboración e implementación de los Planes Institucionales de*

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-07/2019	**Fecha: 03-06-2019**	**Página:** 8/14
Elaborado por: Andre Mitsutake Cueto		

Seguridad de la Información de las entidades del sector público", se acota los siguientes lineamientos:

- *Segmentar la red para los sistemas, servicios informáticos, bases de datos, servidores y grupos de usuarios entre otros.*
- *Las regionales deberán tener un subdominio de red específico.*
- *Se deberá establecer una o varias zonas desmilitarizadas (DMZ) de acuerdo a requerimiento.*

Las siguientes recomendaciones se consideran como buenas practicas para el direccionamiento y segmentación de la red:

- Tener redundancia del servicio de Internet con distintos proveedores.
- La implementación de reglas de filtrado en ICMP.
- Usar rangos de IP's reducidos en el servicio de DHCP.
- Los protocolos de enrutamiento de la entidad cumplan con las mejores prácticas de seguridad.
- Usar NAT (Network Adress Translation) en conexiones necesarias.
- Se recomienda desactivar IPv6 siempre y cuando este protocolo no esté en uso.
- Uso de VLAN's dedicadas para VoIP, el cual mejorara QoS de dicho servicio.

El siguiente punto se debe considerar como un lineamiento si la infraestructura de la entidad tiene la capacidad de implementar este tipo de configuración, de otra manera se recomienda como una buena practica, la cual se menciona en el "*Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público*".

- *Para un uso más eficiente de las redes de datos se recomienda utilizar redes locales virtuales (VLAN).*
- *Se recomienda que servicios de red externos se encuentren en una o varias zonas desmilitarizadas.*

6.2 Seguridad de red perimetral

Una configuración adecuada de la red perimetral debería proteger los sistemas internos de la organización y manejar y controlar de forma segura el trafico que fluye, de acuerdo con una política documentada de acceso a servicios que otorga la institución. En cortafuego es un buen ejemplo de un dispositivo de seguridad perimetral, que por lo general logran un nivel de seguridad adecuado en proporción con riesgos evaluados, con la regla estándar de los cortafuegos que generalmente comienza con la denegación de todo acceso entre las redes internas y externas, y que sigue normas explicitas para satisfacer solo las rutas comunicacionales requeridas.

Como parte fundamental de la seguridad perimetral debe considerarse los siguiente lineamientos:

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-07/2019	**Fecha: 03-06-2019**	**Página:** 9/14
Elaborado por: Andre Mitsutake Cueto		

- Se debe implementar una política de seguridad en la institución sobre conexiones de red. Para cada dispositivo de red perimetral, se debe elaborar una política de seguridad separada de acceso a los servicios. Su contenido se debería aplicar para garantizar que solo se permita el paso de trafico autorizado. Este documento debe contener los detalles de las reglas sobre la puerta de enlace que se requiere administrar y su configuración. Se debe poder definir conexiones permitidas de forma separada según el protocolo de comunicación y otros detalles. De esta forma, para garantizar que solo los usuarios y trafico validos puedan acceder desde las conexiones de comunicaciones, la política debe definir y registrar en detalle las limitantes y reglas aplicadas al trafico que entra y sale por el dispositivo perimetral y los parámetros para su gestión y configuración.
- Se debe aplicar los protocolos de comunicación que utilicen cifrado integrado (Anexo – Protocolos mas usados)
- Se debe habilitar únicamente los puertos de los servicios utilizados por la institución (ingress-filtering)
- Se debe aplicar filtrado con estado (stateful), para evitar conexiones falsificadas en diferentes puertos y/o direcciones IP.

Los siguientes lineamientos propuestos pertenecen a los siguientes lineamientos respectivamente "*Lineamientos y buenas prácticas para la implementación de un Centro de Procesamiento de Datos*" y "*Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público*"

- *Instalar medios de filtrado de comunicaciones del exterior al interior.*
- *De acuerdo a los requisitos de seguridad se deberán implementar y documentar reglas de acceso y salida en los dispositivos de seguridad.*

Como buenas practicas se puede mencionar la implementación de dispositivos y/o software relacionados al filtrado de conexiones externa a internas, algunas mencionadas en el punto *[6.1.1] Infraestructura de Redes,* otras se menciona a continuación.

- Se recomienda emplear sitios conectados duales (redundancia), empleo de distintas rutas

6.3 Seguridad en accesos remotos

El objetivo de estos servicios consiste en permitir el intercambio de datos entre un sitio remoto y un servicio central. Las comunicaciones a través de Internet usan cada vez mas enlaces ADSL, Cable Modem, Red de Telefonía Móvil u otros provistos por un ISP para proporcionar un ancho de banda mayor desde la sede central y uno menor desde el sitio remoto a la sede central. Para la información mas sensible, se debe usar algunas formas canales cifrados tales como el VPN's para entregar seguridad en el intercambio de flujo de datos.

Algunos riegos de seguridad que pueden estar asociados a los servicios de acceso remoto, es el acceso no

autorizado a los sistemas, servicios e información de una organización (eavesdropping), lo que puede llevar a la divulgación, cambios sin autorización o la destrucción de información y/o servicio. También puede llevarse acabo inyección de código malicioso los sistemas, servicios e información de una institución.

- Se debe emplear protocolos de seguridad para la transmisión de información remota, para evitar que ajenos puedan verla o modificarla. Uso de encapsulación tales como VPN/SSL, VPN/IPSec, P2P u otros que mantengan la confidencialidad y privacidad de la información transferida.

6.3.1 Redes Privadas Virtuales(VPN)

Una VPN es una red privada que se implementa al usar infraestructura de redes existentes. Desde el punto de vista del usuario, la VPN se comporta como una red privada y ofrece una funcionalidad y servicios similares. Una VPN se puede usar en diversas situaciones, como para implementar acceso remoto a una organización para empleados móviles o que trabajan fuera de la oficina, comunicar distintos lugares de una organización, lo que incluye enlaces redundantes para aplicar una infraestructura de respaldo, y/o configurar conexiones para la red de una institución a partir de otras instituciones y/o socios comerciales.

La VPN permite que dos computadoras o redes se comuniquen de una forma segura en un medio inseguro (ej. Internet). Esta comunicación emplea sistemas criptográficos para mantener la confidencialidad e integridad de la información transmitida por el canal de enlace.

Existen dos tipos principales de VPN:

- **VPN’s basadas en el cliente**, este tipo de redes VPN permiten tener conectado un usuario a una red remota, a través de una aplicación que se encarga de entablar la comunicación y levantar la VPN. Para acceder a la conexión segura, el usuario debe ejecutar la aplicación y autenticarse con un nombre de usuario y contraseña. De esta manera se crea el canal cifrado entre el equipo y la red remota, para un intercambio seguro de datos.

- **VPN’s basadas en red,** en este enfoque se pretende conectar redes diferentes entres sí a través de una red que no es segura, principalmente Internet. Es el enfoque elegido por empresas para conectar redes de diferentes sedes que se encuentran geográficamente separadas para compartir información de manera segura. Hay varios tipos de redes privadas virtuales de la red. Dentro de este enfoque nos podemos encontrar con los túneles IPSec. Los túneles IPSec son el enfoque más simple de una red VPN y la mayoría de routers y firewalls de red tienen esta característica. Este tipo de enfoque no es más que establecer un túnel (*tunneling*) para que todo el tráfico que se intercambia entre dos redes viaje de manera cifrada. Aunque este mismo enfoque se puede utilizar para encapsular el tráfico para un único dispositivo.

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-07/2019	**Fecha: 03-06-2019**	**Página:** 11/14
Elaborado por: Andre Mitsutake Cueto		

La implementación de los distinto VPN's que existen depende de la funcionalidad que se desea brindar la institución. A continuación se describe los lineamientos respecto a VPN's

- Se debe emplear autenticacion en el uso de comunicación a través de VPN's.
- Se debe emplear ACL para restringir el trafico que fluye a través del enlace VPN (VPN's basadas en red)
- Se debe emplear sistemas criptográficos que no sean vulnerables en comunicaciones VPN's.

Las buenas practicas para la implementación de VPN's recomiendan:

- Implementar protección contra software maliciosos en el punto terminal de la conexión VPN.
- Implementar detección de intrusos, en el punto terminal de la conexión VPN.

6.4 Seguridad en redes Inalámbricas

Las redes inalámbricas se consideran como redes que cubre pequeñas áreas geográficas y usan medios de comunicaciones inalámbricas tales como ondas de radio o infrarrojas. Habitualmente, las redes inalámbricas se usan para implementar una conectividad equivalente a la entrega en LAN y, por lo tanto, también se denominan WLAN. Se destaca que las redes inalámbricas constituyen una categoría distintas de red respecto de aquellas de radio, como GSM, 3G, UHF, VHF,etc. dado que estas emplean torres y otro tipo de infraestructura y protocolo de conmutación de paquetes y/o circuitos.

A continuación los lineamientos a seguir para su utilización:

- Se recomienda emplear estándares IEEE 802.11 para la implementación de medio no físico (inalámbricos) de comunicación.
- Se recomienda emplear estándares IEEE 802.11 y 802.15 para la implementación de tecnologías inalámbricas por medio de espectros visibles, tales como Li-Fi.
- Se debe usar protocolos de seguridad autenticación en redes inalámbricas no vulnerables (WPA2 y WPA3).

Las buenas prácticas recomiendan que las redes inalámbricas:

- Eviten la publicación abierta de los servicios inalámbricos de la institución.
- Emplear el uso de Firewall para redes inalámbricas a partir de la infraestructura corporativa.
- Uso de SNMP con acceso solo a lectura para monitoreo.

6.5 Gestión y monitoreo de redes

Un requisito de seguridad clave para cualquier sistema de red es que sea respaldada por actividades de

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-07/2019	**Fecha: 03-06-2019**	**Página:** 12/14
Elaborado por: Andre Mitsutake Cueto		

gestión de servicios de seguridad, que debe iniciar y controlar la implementación y operación de seguridad. Estas actividades se deberían efectuar para garantizar la seguridad de todos los sistemas de información de una institución.

La gestión de cualquier red se debe emprender de forma segura y por cierto entregar respaldo a toda administración de la seguridad de red. Esto se debe cumplir con especial atención a los distintos protocolos de red disponibles y los servicios de seguridad relacionados.

El monitoreo de la red es un item muy importante en la gestión de la seguridad de la red. La seguridad de la red es un concepto dinámico. El personal de seguridad se debe mantener actualizado en el área y garantizar que todas las redes sigan funcionando con los parches y soluciones mas nuevos de seguridad que entregan los proveedores. Periódicamente se debe tomar medidas para auditar los actuales controles de seguridad, incluidas pruebas de seguridad y verificación de vulnerabilidades.

Los siguiente puntos reflejan los lineamientos para la gestión y monitoreo redes.

- Se debe implementar autenticacion a usuario y contraseña para el acceso a cualquier equipo de comunicación perteneciente a la institución (routers, switch, WiFi, Firewall, etc.)
- Se debe cambiar las contraseñas por defecto de todo equipo de infraestructura de redes
- Se debe implementar contraseñas y cadenas de comunidad apropiadas sobre el protocolo de gestión de redes, si este no es usado deshabilitar el protocolo.
- Se debe contar con políticas que definan explícitamente la responsabilidad, accesos y otros que fueran necesarios para todo personal involucrando en la administración y uso de la infraestructura de redes de la institución.

Los lineamientos a mencionar se encuentra plasmados en el "*Lineamiento y buenas practicas para la implementación de un Centro de Procesamientos de Datos".*

- *Contar con diagramas de red actualizados.*

- *Documentar de forma apropiada las configuraciones actuales de los equipos de comunicación.*
- *Documentar la información de los equipos de comunicación, incluyendo las especificaciones técnicas, físicas, lógicas e información de los contenidos.*

Los siguientes controles mencionados en el "*Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público*", se plasman como lineamientos.

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-07/2019	**Fecha: 03-06-2019**	**Página:** 13/14
Elaborado por: Andre Mitsutake Cueto		

- *Establecer un reglamento para la gestión de la red.*
- *Elaborar procesos/procedimientos para la gestión de la infraestructura de red.*
- *Se deberán elaborar y actualizar periódicamente los diagramas de red y documentar la arquitectura de la red.*
- *Establecer las condiciones de uso aceptable de Internet, considerando restricciones para la conexión a Internet, siguiendo el principio del mínimo privilegio que garantice la calidad de servicio.*

Como buenas practicas se puede recomendar:

- El monitoreo constante de la infraestructura de redes dado que es factor importante a considerar en los servicios de la institución para garantizar su disponibilidad, esto facilita tomar las acciones pertinentes en caso de problemas, registrándolos y alertando a los administradores del servicio para poder aplicar acciones correctivas y tener un informe estadístico de incidencias en un lapso determinado de tiempo.

- El almacenamientos de registros de eventos (logs), para la revisión y comprobación de las acciones realizadas para reconstruir una serie de eventos que generaron un hecho específico. La manera más común para efectuar este tipo de auditorías es a través de registros de eventos (logs) en servidores seguros y solamente accesibles por personal autorizado.

- Utilizar siempre los registros de eventos con toda la información posible. En este marco, lo mínimo que deberían contener son: información sobre la hora que se ha producido el evento; fecha, hora , minuto y segundo, categorización del evento; indicando la importancia o impacto sobre el sistema, e información descriptiva la cual corresponde a la información sobre el evento acontecido.

- Documentar en informes post-mortem las acciones correctivas que se tomaron en caso de cualquier suceso que haya afectado al servicio, con la finalidad de que si los mismos sucesos se repitieran, estos se resuelvan fácilmente.

- Utilizar un centralizador de registros de eventos para facilitar su administración y posterior análisis.

- Realizar una capacitación periódica, al menos de forma anual, para que el personal de Tecnologías de la Información (TI) esté debidamente calificado en el manejo de los equipos de redes.

- Establecer las funciones y contenidos de los equipos de redes de acuerdo a los tipos de información y usos, implementando un catálogo o clasificación de los mismos.

- Planificar las actualizaciones (firmware u otros) y mejoras de los equipos de redes.

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-07/2019	**Fecha: 03-06-2019**	**Página:** 14/14
Elaborado por: Andre Mitsutake Cueto		

- Obtener información oportuna sobre vulnerabilidades técnicas, para la evaluación de exposición de estas vulnerabilidades de la red de la institución hacia el Internet.

ANEXO

Buenas Practicas
Deshabilitar servicios innecesarios
Cambio de contraseñas por defecto
Implementar contraseñas robustas
Realizar respaldo y/o actualizar firmware
Deshabilitar protocolos de administracion que no usen cifrado (ej.: Telnet, FTP)
Restringir acceso físico al equipo
Implementar un acceso seguro a la terminal del equipo, entrada auxiliar y/o terminales virtuales.

DESIGNACIÓN DE PUNTOS A DESARROLLAR:

- Propuesta de descripciones por punto (Aldo – APS).
- Seguridad MAN/WAN (Dennis – BCB).
- Seguridad de servicios/aplicaciones Anexo#7 PISI (Grover – AJ).
- Acuerdos de confidencialidad intercambio de información entre entidades (Lin. Interoperabilidad) (Roni Oyardo – EASBA).

ACUERDOS Y COMPROMISOS:

- Revisión del documento, aportes y observaciones (Todos).
- Toda observación hasta el 14 de Junio de 2019. Siguiente reunión 17 de Junio de 2019.