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-05/2019	**Fecha: 13-05-2019**	**Página:** 1/10
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 (Glosario – definiciones, protocolos mas usados).
2. Revisión y comentarios de propuestas para Diseño de Redes y Referencia en otros lineamientos.
3. Análisis de propuestas y observaciones.
4. Aprobación de redacciones.
5. Designación de puntos para desarrollar.
6. Acuerdos para la siguiente reunión.

DESARROLLO:

1. Revisión

- **Glosario-definiciones (Aprobado)**

  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.

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-05/2019	**Fecha: 13-05-2019**	**Página:** 2/10
Elaborado por: Andre Mitsutake Cueto		

- **Protocolos mas usados (Aprobado)**

Lineamientos

Protocolo	Servicios	Alternativa Protocolo-Puerto Seguro
- HTTP (Hypertext Transfer Protocol) [TCP: 80, 8080, Otros]	- Sistemas Transaccionales - Servicios Web - Webmail - Otros	- HTTPS (Hypertext Transfer Protocol Secure) - TLS 1.3 (Transport Layer Security) - RFC 8446 - HSTS (HTTP Strict Transport Security)- RFC 6797 [TCP: 443, 8443]
- FTP (File Transfer Protocol) [TCP: 20,21] - Telnet [TCP:23]	- Transferencia de archivo - Acceso remoto - Otros	- SFTP (SSH File Transfer Protocol) - SSH (Secure Shell) - SCP (Secure Copy Protocol) [TCP: 22]

Buenas Practicas

Protocolo	Servicios	Alternativa Protocolo-Puerto Seguro
- SMTP (Simple Mail Transfer Protocol) [TCP: 25] - POP3 (Post Office Protocol) [TCP: 110] - IMAP (Internet Message Access Protocol) [TCP: 143]	- Protocolos de Correo Electronico	- SMTPS (Simple Mail Transfer Protocol Secure) – RFC 8314 [TCP: 465] - POP3+SSL (Post Office Protocol) – RFC 2595 [TCP: 995] - IMAP+SSL (Internet Message Access Protocol) – RFC 2595 [TCP: 993]
LDAP (Lightweight Directory Access Protocol) [TCP: 389]	- Servicio de autenticacion y directorios	LDAPv3+TLS (Lightweight Directory Acccess Protocol) – RFC 2830 [TCP: 993]
DNS (Domain Name System) [TCP/UDP: 53]	- Sistema de nombre de dominios	DNSSEC (Domain Name System Security Extensions) RFC 4033, RFC 4034, and RFC 4035 [TCP/UDP: 53] Nota: recomendación para la actualización de los registros de DNS con los servidores de la ADSIB, actualmente la ADSIB están realizando pruebas para su implementación.
SNMP (Simple Network Management Protocol) [UDP: 161,162]	- Administracion y modificacion de equipos de red	SNMPv3 (Simple Network Management Protocol) RFC 3411, RFC 3418 [UDP:10161,10162]

2. Propuestas

- Diseño de Redes

Lineamientos

- Requisitos mínimos que se debe tener en la infraestructura de redes:
  Dispositivo de protección perimetral
  Uso de Switch’s en vez de HUB’s
- 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.
- Se debe identificar y/o etiquetar de forma apropiada todos los equipos de redes, según la nomenclatura adoptada por la institución.
- Se debe generar la documentación referida a manuales de operación y hojas de datos de los equipos de redes, incluyendo las especificaciones técnicas físicas y lógicas e información de los contenidos.
- 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.
- ***Lineamientos y buenas prácticas para la implementación de un Centro de Procesamiento de Datos***
- ***Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad***

de la Información de las entidades del sector público

- 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

Buenas Practicas

- Se recomienda 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.

- Se recomienda 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.

- Se recomienda 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.

- Se recomienda 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, y información descriptiva la cual corresponde a la información sobre el evento acontecido.

- Se debe 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.

- Se recomienda utilizar un centralizador de registros de eventos para facilitar su administración y posterior análisis.

- Se recomienda realizar una capacitación periódica, al menos de forma anual, para que el personal 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-05/2019	**Fecha: 13-05-2019**	**Página:** 4/10
Elaborado por: Andre Mitsutake Cueto		

Tecnologías de la Información (TI) esté debidamente calificado en el manejo de los equipos de redes.

- Se recomienda 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.
- Se recomienda planificar las actualizaciones (fimware u otros) y mejoras de los equipos de redes.
- Se recomienda la implementación de Sistemas de Detección de Intrusos (IDS) y/o Sistemas de Prevención de Intrusos (IPS) en la institución correspondiente.

- **Otros Lineamientos**
- **Lineamientos y buenas prácticas para la implementación de un Centro de Procesamiento de Datos**

5.4.3 Equipamiento de comunicación

Los equipos de comunicación son aquellos que proveen el servicio de telecomunicaciones con el fin de que los usuarios se comuniquen utilizando los servicios y aplicaciones informáticas propias de la institución.
A continuación, los lineamientos técnicos a seguir para los equipos de comunicación:

- Contar con diagramas de red actualizados.
- Realizar un inventario de equipos de comunicación y puntos de conexión dentro del CPD que sea permanentemente actualizado.
- Identificar y etiquetar de manera apropiada todo el equipamiento, medios de distribución y accesorios empleados en la implementación.
- Segmentar la planificación lógica según las necesidades de la institución.
- Instalar medios de filtrado de comunicaciones del exterior al interior.
- 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

Como buenas prácticas para los equipos de comunicación se recomienda que:

- 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.
- Se realicen sesiones de capacitación periódicas, de manera tal que el personal de TI sea capacitado en el manejo de los equipos de comunicación.
- Instalen tecnología de alto tráfico en transmisión de datos para los enlaces de backbone (fibra óptica, cobre certificado u otros).

5.4.3.1 Cableado de conexión a equipos terminales (TODO)

Es el cableado que interconecta a equipos terminales de uso desde los ambientes de un mismo piso.

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-05/2019	**Fecha: 13-05-2019**	**Página:** 5/10
Elaborado por: Andre Mitsutake Cueto		

Los siguientes puntos reflejan los lineamientos para la instalación del cableado horizontal:

- 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.
- Todo el cableado de conexión de equipos terminales debe estar apropiadamente identificado y/o etiquetado, según la nomenclatura adoptada por la institución.

Las buenas prácticas para la instalación de cableado horizontal recomiendan:

- 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.

5.4.3.2 Cableado entre diferentes niveles (TODO)

Es el cableado que une las diferentes plantas en un edificio o en varios edificios, también se le conoce como backbone. Estas instalaciones pueden ser interiores al edificio (Indoor) o exteriores (Outdoor).
Los lineamientos para la instalación del cableado vertical establecen que:

- 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.
- Es necesario respetar la longitud máxima del tendido de cableado estructurado de acuerdo a la tecnología utilizada.

Como buenas prácticas de cableado vertical, se recomienda:

- Instalar la protección apropiada a los medios de transmisión empleados.
- El cableado vertical debe realizar su recorrido por un shaft independiente.
- Identificar y/o etiquetar de forma apropiada todo el cableado entre los diferentes niveles, según la nomenclatura adoptada por la institución.

5.4.3.3 Escalerillas para el cableado (TODO)

Las escalerillas sirven de transporte para el cableado estructurado de datos, basado en escalerillas metálicas ligeras adjuntas a lo largo del recorrido.
A continuación los lineamientos a seguir para su utilización:

- 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.
- Contar con los planos actualizados de la distribución de las escalerillas utilizadas en el CPD.
- Si se utilizan escalerillas aéreas, estas deberán estar instaladas de tal forma que no caigan al suelo de ninguna manera, inclusive cuando sean cargadas por el peso del cableado. Deberán estar construidas con materiales resistentes y no susceptibles a oxidación.
- En caso de utilizar escalerillas de piso, estas deberán estar fijadas fuertemente al piso con el fin de no moverse cuando se ejecuten las tareas de cableado.

Las buenas prácticas recomiendan que el sistema de escalerillas:

- Debe estar listo para permitir un crecimiento del 40% en el cableado de datos.
- Debe estar construido en material metálico y galvanizado.
- Debe estar conectado al sistema de puesta a tierra eléctrico del CPD.
- Debe cumplir estándares de instalación internacionales. Los estándares están referidos en la bibliografía anexa.
- No debe perjudicar el flujo de aire en el CPD.

5.4.3.4 Accesorios y complementos para equipos de comunicación (TODO)

Los siguientes puntos reflejan las buenas prácticas recomendadas para el uso de accesorios y complementos de los equipos de comunicación:

- 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.
- 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

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-05/2019	**Fecha: 13-05-2019**	**Página:** 7/10
Elaborado por: Andre Mitsutake Cueto		

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.

Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público.

Anexos

7. Seguridad de las comunicaciones

Establecer controles que permitan proteger la información transmitida a través de las redes de telecomunicaciones reflejada en documentos.

7.1. Gestión de la seguridad en redes

Garantizar la protección y la disponibilidad de la Información en las redes de datos.

7.1.1. Gestión de la red

A. Objetivo

Gestionar y administrar las redes de datos y la información en tránsito por este medio.

B. Aplicabilidad Redes de datos.

C. Directrices

I. Establecer un reglamento para la gestión de la red.
II. El reglamento debe considerar roles y responsabilidades, procedimientos, requisitos de seguridad, tipos, métodos de autenticación, monitoreo, autorización para acceso acorde al control de accesos y administración de la infraestructura de red.
III. Considerar la implementación de dispositivos de red redundantes para puntos de fallo único donde la disponibilidad sea un factor crítico.
IV. Elaborar procesos/procedimientos para la gestión de la infraestructura de red.
V. Implementar controles para el resguardo de la integridad, confidencialidad, disponibilidad, no repudio y trazabilidad de la información transmitida al interior y exterior de la entidad o institución pública.
VI. El cableado de red a nivel de núcleo, distribución y acceso deberá estar identificado, etiquetado y ser operativo.
VII. Se deberán elaborar y actualizar periódicamente los diagramas de red y documentar la arquitectura de la red.
VIII. 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.
IX. Restringir el ancho de banda para recursos de alto consumo acorde al puesto laboral.

7.1.2. Seguridad en servicios de red

A. Objetivo

B. Aplicabilidad

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-05/2019	**Fecha: 13-05-2019**	**Página:** 8/10
Elaborado por: Andre Mitsutake Cueto		

Servicios de red internos y externos.
C. Directrices

I. Implementar controles de conexión, autenticación y cifrado para los servicios de red.
II. En función de las necesidades de protección de confidencialidad de la información, considerar la implementación de controles para la comunicación segura en servicios de red.
III. Se recomienda que servicios de red externos se encuentren en una o varias zonas desmilitarizadas.

7.1.3. Seguridad en la red perimetral

A. Objetivo
Proteger la infraestructura de red interna ante amenazas que se originan de redes ajenas y/o públicas.
B. Aplicabilidad
Infraestructura de red.
C. Directrices

I. Implementar controles de seguridad perimetral que protejan la red ante posibles intrusiones.
II. De acuerdo a los requisitos de seguridad se deberán implementar y documentar reglas de acceso y salida en los dispositivos de seguridad.
III. Establecer una o varias zonas desmilitarizadas (DMZ).
IV. Se deberán implementar reglas de control de salida y registro según corresponda.
V. Se deberá monitorear regularmente la actividad en las redes de datos.
VI. Se deberán implementar protocolos de conexión segura.
VII. Se deberán implementar, cuando se vea necesario, parámetros técnicos de encriptación para conexiones seguras y reglas de seguridad.

7.1.4. Segmentación de la red

A. Objetivo
Separar la red en subredes de acuerdo a requerimiento institucional.
B. Aplicabilidad
Red institucional, sistemas, servicios, bases de datos, servidores y grupos de usuarios entre otros.
C. Directrices

I. Segmentar la red para los sistemas, servicios informáticos, bases de datos, servidores y grupos de usuarios entre otros.
II. Para un uso más eficiente de las redes de datos se recomienda utilizar redes locales virtuales (VLAN).
III. Las regionales deberán tener un subdominio de red específico.
IV. Segmentar las salidas de internet relacionadas con el consumo interno de servicios.
V. Se deberán segmentar el dominio institucional interno (DNS interno) del dominio institucional externo (DNS externo).
VI. Se deberá establecer una o varias zonas desmilitarizadas (DMZ) de acuerdo a requerimiento.

7.1.5. Seguridad en redes WiFi

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-05/2019	**Fecha: 13-05-2019**	**Página:** 9/10
Elaborado por: Andre Mitsutake Cueto		

A. Objetivos
Gestionar la seguridad de redes WiFi.
B. Aplicabilidad
Redes WiFi.
C. Directrices

I. Comunicar e informar las redes WiFi oficiales y autorizadas para uso.
II. Concientizar sobre el uso seguro de las redes WiFi, que informe sobre los riesgos de conexión a redes desconocidas y no autorizadas.
III. Implementar una red virtual local dedicada para redes WiFi diferente a la red cableada.
IV. Filtrar el acceso a la red WiFi por dirección MAC, servidor proxy o cualquier otro método de acuerdo al reglamente de gestión de la red de comunicaciones.
V. Utilizar algoritmos de cifrado robustos en las redes WiFi.

7.2. Seguridad del servicio de mensajería electrónica
Gestionar de forma eficiente y segura el servicio de mensajería y/o correo electrónico.
7.2.1. Mensajería y correo electrónico
A. Objetivo
Asegurar la disponibilidad, integridad y confidencialidad de la información transmitida a través de estos servicios.
B. Aplicabilidad
Mensajería y correo electrónico institucional.
C. Directrices

I. Elaborar un reglamento de uso aceptable del correo electrónico institucional.
II. El reglamento debe establecer reglas de uso del servicio de correo electrónico y mensajería.
III. El servicio de correo electrónico deberá ser independiente y pertenecer a un dominio institucional, evitando el uso de correos comerciales.
IV. El servicio de correo electrónico deberá implementarse en un servidor independiente.
V. Utilizar técnicas de autenticación robustas, además de control a las redes de acceso público.
VI. Las cuentas de usuario deberán ser autenticadas para prevenir y controlar la suplantación de correo electrónico.
VII. Utilizar protocolos y puertos seguros para la configuración del servicio de correo electrónico.
VIII. Gestionar regularmente el almacenamiento de correo electrónico basura.
IX. Se deberán establecer la restricción de uso para archivos adjuntos.
X. Se deberá instalar software anti-spam.

7.3. Control sobre información transferida
Asegurar la información transferida.

7.3.1. Transferencia de información

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-05/2019	**Fecha: 13-05-2019**	**Página:** 10/10
Elaborado por: Andre Mitsutake Cueto		

A. Objetivo
Preservar la integridad y confidencialidad de la información transferida.
B. Aplicabilidad
Información institucional transferida.
C. Directrices

I. Definir los requisitos de seguridad para la transferencia de información de acuerdo a la criticidad y sensibilidad de la misma.
II. Elaborar procesos/procedimientos orientados a prevenir la interceptación, manipulación, duplicación, repetición, descubrimiento no autorizado y destrucción de la información transferida en cualquier medio.
III. Utilizar técnicas de cifrado para transferencia de información sensible y crítica.
IV. Se deberá firmar un acuerdo de confidencialidad para la transferencia de la información entre partes, de acuerdo a la criticidad y sensibilidad de la misma.

DESIGNACIÓN DE PUNTOS A DESARROLLAR:

- Glosario y definiciones (revisión de los términos hasta ahora avanzados) → André Mitsutake.
- Desarrollo de anexos para la implementación de los lineamientos en pequeñas y medianas instituciones → Hernán Enríquez.

ACUERDOS Y COMPROMISOS:

- Revisión de los puntos y lineamientos del PISI y CPD (página web del CTIC) para su selección en buenas prácticas y/o lineamientos específicos por parte de todos los miembros de la mesa (hasta el jueves 16 de mayo 23:59).