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-08/2019	**Fecha: 01-07-2019**	**Página:** 1/8
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 (Aldo-APS, Seguridad MAN/WAN, Seguridad de servicios/aplicaciones Anexo#7 PISI; Grover-AJ, Acuerdos de confidencialidad intercambio de información entre entidades Roni Oyardo - EASBA).
2. Análisis de propuestas y observaciones.
3. Aprobación de redacciones.
4. Designación de puntos para desarrollar.
5. Acuerdos para la siguiente reunión.

DESARROLLO:

1 Revisión y comentarios

1.1 Acuerdo de confidencialidad intercambio de información entre entidades (Roni Oyardo – EASBA)
NOTA: *Tomar en cuenta lineamiento de interoperabilidad Capitulo 5 Naturaleza del servicio de interoperabilidad y 8 Seguridad (redes)*
1.2 Seguridad MAN/WAN (Dennis – BCB)
SEGURIDAD MAN/WAN
Estos dos términos tendrían que ir en la parte de los conceptos.

- WAN – Redes de área amplia, utilizados para la interconexión de dispositivos dentro y/o fuera del territorio de un país. Ejemplos de tecnologías utilizadas en este tipo de redes son: enlaces serial, frame relay, MPLS, Satelital y otros.
- MAN – Redes de área metropolitana, utilizados para la interconexión de dispositivos dentro de una ciudad. Ejemplos de tecnologías utilizadas en este tipo de redes son: enlaces ethernet, fibra óptica, Wireless, Wimax, y otros.

Con el fin de proteger la confidencialidad, integridad y disponibilidad de la información transmitida por redes MAN y WAN, en estas tecnologías utilizadas para transportar el tráfico de la red se establecen las siguientes buenas prácticas:

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-08/2019	**Fecha: 01-07-2019**	**Página:** 2/8
Elaborado por: Andre Mitsutake Cueto		

Protección de la confidencialidad e integridad.- Para proteger los datos de intentos de intercepción y/o manipulación del tráfico de red transportado en redes MAN & WAN, se deben implementar tecnologías de cifrado en el canal de comunicación, a través de uso de VPNs como por ejemplo VPN IPSEC, VPN SSL, L2TP, PPTP u otros siempre y cuando utilicen estándares/protocolos abiertos.

Protección de la disponibilidad.- De acuerdo al grado de criticidad del enlaces para las operaciones de la empresa/institución se debe contemplar el establecimiento de un canal de comunicación de respaldo alterno, el cual no debe ser contratado al mismo proveedor del enlace principal, o en caso de que se realicen instalaciones propias de estos enlaces de respaldo deben tener una trayectoria física distinta al enlace principal. De igual manera a los enlaces de respaldo se les deberá proveer de protección en el cifrado del canal de comunicación.

Acuerdos de confidencialidad.- En caso de por razones del negocio se requiera establecer enlaces de comunicación con terceras partes (con otras instituciones públicas, empresas públicas, empresas privadas, organizaciones y otros que sean ajenos a la misma institución/empresa pública), para estos tipos de enlaces se deben tener acuerdos de confidencialidad, en los cuales se contemple la protección del medio de comunicación a través del uso de criptografía (cifrado). A su vez este acuerdo de confidencialidad debe mencionar a la tercera parte que el medio de comunicación debe ser utilizado de manera exclusiva y no dar acceso a través del mismo medio a otras terceras partes (subarrendamiento).

Enlaces a través de internet.- Actualmente el establecimiento de tuneles a través de internet están siendo utilizados como alternativas de canales de comunicación para conexiones WAN/MAN por diferentes factores. En este sentido se establece como lineamiento que el uso de los túneles establecidos por internet para la comunicación WAN/MAN deben ser canales cifrados con el uso de VPNs, cifrando el paquete en su totalidad y no sólo las cabeceras del paquete a ser transportado por estos medios.

2. Análisis de propuestas, observaciones y aprobaciones
2.1 Modificación de redacción
2. Objetivo (Aprobado)
Establecer lineamientos y buenas practicas de seguridad en las etapas de diseño, implementación, monitoreo y mejoras de redes de telecomunicaciones, identificando y analizando los factores de riesgos que se debería considerar al momento de establecer la seguridad en los distintos tipos de conexiones y sistemas de redes.

3. Alcance y ámbito de aplicación (Aprobado)

El alcance de los lineamientos y buenas practicas para la implementación o adecuación, administración y mantenimiento de la seguridad en redes en todas las entidades del sector público del Estado Plurinacional de Bolivia.

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-08/2019	**Fecha: 01-07-2019**	**Página:** 3/8
Elaborado por: Andre Mitsutake Cueto		

En cuanto al ámbito de aplicación, todas las entidades con un estándar, norma o buena práctica ya implementado en el ámbito de seguridad de redes, serán aceptadas siempre y cuando estén documentadas y alineadas a este documento.

!!!=> No se tiene definido donde se ubicara el párrafo que hace referencia a que el lineamientos actual es un complemento de PISI ????

Marco normativo referencial (PISI)
Este documento debe ser tomado como un complemento de “Los Lineamientos del Plan Institucional de Seguridad de la Información” - ANEXO#7 – PISI

4. Marco normativo referencial
!!!=> El marco normativo referencial debera citar a la norma del PISI (la cual cubre a las demas) revisar si alguna normativa se encuentra fuera del alcance de la norma del PISI???

La elaboración del presente documento se enmarca en el mandato institucional respaldado por:

- El artículo 22 del Decreto Supremo N° 29894, de 7 de febrero de 2009, inciso t), de Organización del Órgano Ejecutivo, que establece que: “El Ministerio de la Presidencia es el ente rector de Gobierno Electrónico y de Tecnologías de Información y Comunicación para el sector público del Estado Plurinacional de Bolivia, siendo el encargado de establecer las políticas, lineamientos y normativa específica para su implementación, seguimiento y control”.

El Decreto Supremo Nº 2514, de 9 de septiembre de 2015, en sus siguientes incisos:

- Artículo 2, de creación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC), como “una institución pública descentralizada de derecho público, con personalidad jurídica, autonomía de gestión administrativa, financiera, legal y técnica y patrimonio propio, bajo tuición del Ministerio de la Presidencia”.

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-08/2019	**Fecha: 01-07-2019**	**Página:** 4/8
Elaborado por: Andre Mitsutake Cueto		

- Artículo 9, párrafo I, de creación del: "Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia (CTICEPB), como instancia de coordinación para la implementación de Gobierno Electrónico y para el uso y desarrollo de Tecnologías de Información y Comunicación".
- Artículo 11, que establece como parte de las funciones del CTIC-EPB: "a) Formular propuestas de políticas y normativa relacionada con Gobierno Electrónico, a ser presentadas a la AGETIC" y "b): Presentar proyectos y programas de Gobierno Electrónico y Tecnologías de Información y Comunicación en el ámbito gubernamental a la AGETIC para su gestión.

- Artículo 7, que enumera entre las funciones de la AGETIC: "f) Establecer los lineamientos técnicos en seguridad de información para las entidades del sector público" e "i) Elaborar, proponer, promover, gestionar, articular y actualizar el Plan de Implementación de Gobierno Electrónico y el Plan de Implementación de Software Libre y Estándares Abiertos para las entidades del sector público; y otros planes relacionados con el ámbito de gobierno electrónico y seguridad informática".

El respaldo normativo específico concerniente al Plan de Contingencia Tecnológica incluye:

- El artículo 5 de la Ley N° 164, de 8 de agosto de 2011, Ley General de Telecomunicaciones, que establece como uno de los principios del sector de telecomunicaciones y TIC a la continuidad: "Los servicios de telecomunicaciones y tecnologías de información y comunicación, así como el servicio postal, deben prestarse en forma permanente y sin interrupciones, salvo los casos previstos por norma".

- El artículo 164 (Continuidad del servicio), del Decreto Supremo N° 1391 de Reglamento General de la Ley 164 de Telecomunicaciones, que señala que: "Sin perjuicio de los derechos establecidos en la Ley Nº 164, cuando la ATT tramite reclamaciones, respecto a los servicios de telecomunicaciones disponibles al público; previo análisis podrá ordenar al operador o proveedor que mantenga el servicio o que, en el plazo que el indique, proceda a su re-conexión, según corresponda, mientras resuelva el reclamo presentado".

Los siguientes artículos del Decreto Supremo N° 1793, de Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, de 13 de noviembre de 2013:

- Artículo 3 (Definiciones) Parágrafo VI. Respecto a la seguridad informática:

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-08/2019	**Fecha: 01-07-2019**	**Página:** 5/8
Elaborado por: Andre Mitsutake Cueto		

a. Seguridad informática: Es el conjunto de normas, procedimientos y herramientas, las cuales se enfocan en la protección de la infraestructura computacional y todo lo relacionado con ésta y, especialmente, la información contenida o circulante.
b. 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.

c. 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.

- Artículo 4 (Principios) Parágrafo II. Tratamiento de datos personales, Inciso d) Seguridad: “Se debe implementar los controles técnicos y administrativos que se requieran para preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información, brindando seguridad a los registros, evitando su falsificación, extravío, utilización y acceso no autorizado o fraudulento”.

- Artículo 8 (Plan de contingencia), que establece que: “Las entidades públicas promoverán la seguridad informática para la protección de datos en sus sistemas informáticos, a través de planes de contingencia desarrollados e implementados en cada entidad”.

5. Términos y definiciones

!!!=> En terminos y definiciones no se debera considerar terminos y deficiones de otros lineamientos, se debe realizar el agrupamientos de todos los terminos y unicamente citar los que no es encuentra en los demas lineamientos.

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.

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-08/2019	**Fecha: 01-07-2019**	**Página:** 7/8
Elaborado por: Andre Mitsutake Cueto		

- 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. Desarrollo
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 fundamental.

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 para la mejora de seguridad de redes.

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

6.1 Diseño de Seguridad en Redes
6.2 Implementación de Seguridad de Redes
6.2.1 Seguridad de red perimetral
6.2.2 Seguridad en accesos remotos
6.2.3 Seguridad en redes Inalámbricas
6.3 Gestión y monitoreo de redes
6.4 Mejoras en seguridad de redes de telecomunicaciones

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-08/2019	**Fecha: 01-07-2019**	**Página:** 8/8
Elaborado por: Andre Mitsutake Cueto		

DESIGNACIÓN DE PUNTOS A DESARROLLAR:

- Revisión de los términos y definición (Andre Mitsutake)
- Revisión del Marco Normativo Referencial (Solo PISI - Paty)

ACUERDOS Y COMPROMISOS:

- Aporte de la estructura del Documento del Desarrollo. (TODOS)
- 08 de Julio de 2019 novena reunión