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-02/2019	**Fecha: 15-04-2019**	**Página:** 1/8
Elaborado por: Andre Mitsutake Cueto		

ASISTENTES:

De acuerdo a la lista adjunta.

AGENDA DE TRABAJO:

1. Revisión y comentarios de propuestas sobre Objetivos, Alcance y ámbito de aplicación, temas/tópicos.
2. Revisión y comentarios sobre Marco teórico referencia,Términos y definiciones.
3. Análisis de propuestas de seguridad en capa física.
4. Aprobación de redacciones.
5. Designación de puntos para desarrollar.
6. Acuerdos para la siguiente reunión.

DESARROLLO:

2. Marco Normativo Referencial

[Opción 1 AGETIC]
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”.

- Artículo 9, párrafo I, de creación del: “Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia (CTIC-EPB), 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

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-02/2019	**Fecha: 15-04-2019**	**Página:** 2/8
Elaborado por: Andre Mitsutake Cueto		

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:

  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.

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-02/2019	**Fecha: 15-04-2019**	**Página:** 3/8
Elaborado por: Andre Mitsutake Cueto		

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”.

3. Objetivo
[Opción 1]
Establecer lineamientos para incorporar buenas practicas de seguridad en las etapas de diseño, implementación y operación de redes de telecomunicaciones.

[Opción 2 - Aprobado]
El presente documento tiene como objetivo establecer lineamientos, para incorporar buenas prácticas de seguridad en las etapas de diseño, implementación y operación de telecomunicaciones, identificando y analizando los factores de comunicación que se debería considerar al momento de establecer los requisitos de seguridad de redes en los distintos tipos de conexiones, sistemas y potenciales riesgos.

4. Alcance y ámbito de aplicación - aprobado

El alcance de los lineamientos contenidos en este documento establecen los estándares 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.

[Opción 1 - aprobado]
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.

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-02/2019	**Fecha: 15-04-2019**	**Página:** 4/8
Elaborado por: Andre Mitsutake Cueto		

[Opción 2]
Sin perjuicio de lo desarrollado por aquellas que hayan asumido normas, estándares y/o buenas prácticas internacionales y/o nacionales que no entren en conflicto con el lineamiento actual, que se encuentren vigentes o de otra naturaleza en materia de redes.

Establecer lineamientos para definir parámetros mínimos en el diseño, implementación y operación en las capas de acceso, red, transporte y aplicación de redes de telecomunicaciones.

5. Términos y definiciones
[Opcion 1 AGETIC]

- 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: (agregar)

- Redes: (agregar)

- MTD: (Tiempo máximo de inactividad tolerable) Es el máximo tiempo tolerable sin servicio o caída de servicio que una entidad puede soportar para cumplir con sus objetivos planteados, sin que se produzcan efectos irreversibles. También hace referencia al tiempo durante el cual el proceso identificado puede ser inoperable hasta que la entidad empiece a tener pérdidas y colapse.

- 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.

- RTO: (Tiempo Objetivo de Recuperación): Es el periodo de tiempo real dentro del cual la entidad debe recuperarse después de una interrupción. También hace referencia al tiempo transcurrido entre la interrupción y recuperación e indica el tiempo disponible para recuperar lo interrumpido.

- RPO: (Punto Objetivo de Recuperación): Es la tolerancia o sensibilidad que tienen los procesos críticos de la entidad para su operación, respecto a la pérdida de información sensible. Hace referencia también al rango de tolerancia que la entidad tiene en relación con la pérdida de datos o información y eventos de desastre.

- 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.

6. Lineamientos Para la Elaboración de Seguridad de Redes (agregar una aclaración respecto a las instituciones que aplican algún estándar internacional)
[Modelo OSI, estructura referencial para el análisis de seguridad de redes]
######################
[8] Diseño de red
[7]Aplicación
[6]Presentación
[5]Sesión
[4]Transporte
[3]Red
[2]Enlace de Datos
[1]Capa Física

######################

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-02/2019	**Fecha: 15-04-2019**	**Página:** 6/8
Elaborado por: Andre Mitsutake Cueto		

[Opción 1 AGETIC- Temario tentativo]
[6.1] Sistemas de redes de Área Local - LAN
[6.2] Conexiones de los ISP's
[6.3] Sistemas de redes inalámbricas
[6.4] Puertas de enlace (gateways)
[6.5] Redes privadas virtuales (VPN)
[6.6] Controles de seguridad técnicas

[1] Capa Física
Ethernet (IEEE 803)
La intención de estos estándares es proporcionar una serie de prácticas recomendadas para la terminación de cableado que soporten una amplia variedad de los servicios existentes, y la posibilidad de soportar servicios futuros que sean diseñados considerando los estándares de cableado.

TIA/EIA 568 A:
• Requerimientos mínimos para cableado de telecomunicaciones dentro de un ambiente de oficina.
• Topologías y distancias recomendadas.
• Parámetros de medios de comunicación que determinan el rendimiento.

TIA/EIA 568 B:
- (Punto a desarrollar)

Propósito del estándar TIA/EIA 568-A:
• Establecer un cableado estándar genérico de telecomunicaciones para respaldar un ambiente multiproveedor
• Permitir la planeación e instalación de un sistema de cableado estructurado para construcciones comerciales.
• Establecer un criterio de ejecución y técnico para varias configuraciones de sistemas de cableados .
• Proteger las inversiones realizadas por el cliente (como mínimo 10 años)
• Las normas TIA/EIA fueron creadas como norma de industria en un país pero se han empleado como normas internacionales por ser las primeras en crearse.

Propósito del estándar TIA/EIA 568-B:

Vulnerabilidades
TAP's.

Inalámbricas (agregar Light-Fi)
IEEE 802.11x

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-02/2019	**Fecha: 15-04-2019**	**Página:** 7/8
Elaborado por: Andre Mitsutake Cueto		

- 802.11 2Mbps [2.4GHz]
- 802.11a 54 Mbps [5GHz]
- 802.11b 11Mbps [2.4GHz]
- 802.11g 54Mbps [2.4GHz]
- 802.11n 100 – 600 Mbps [2.4GHz / 5GHz]

Recomendaciones para el alcance de la señal de Wi–Fi dentro de la entidad:
Es recomendable considerar la distancia de cobertura del servicio de Wi-Fi, que esté limitado a la infraestructura de la entidad.

agregar Light–Fi

[2] Capa enlace de datos

- Registro de direcciones MAC (buenas prácticas)
- Mitigación de Broadcast (capa 3)
- Seguridad en STP, VTP
- 802.1x (autenticación, radius y diameter)
- Limitación de troncales para VLAN (VTP 802.1q)

Registro de direcciones MAC-aprobado:

Se deberá 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 deberá 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.

Se recomienda implementar un STP cuando se tenga una estructura de red local amplia. (buena práctica)

Se recomienda implementar el protocolo 802.1x conforme a la cantidad de registros de direcciones MAC de la entidad. (buena práctica)

Se recomienda limitar el uso de las redes troncales VLAN’s de la red local de la entidad. (buena práctica)

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-02/2019	**Fecha: 15-04-2019**	**Página:** 8/8
Elaborado por: Andre Mitsutake Cueto		

Se deberá tener una red segmentada para el acceso a invitados y personal eventual. (buena práctica – revisar capa 3)

Se recomienda no publicar el SSID de la red Wi-Fi de la entidad. (buena práctica – revisar capa 3)

El registro e implementación de control de direcciones MAC de equipos pertenecientes a la red de interoperabilidad del Estado Plurinacional de Bolivia es obligatorio y dependiente de los accesos a la información que tenga.
Las instituciones pertenecientes a la red de interoperabilidad del Estado Plurinacional de Bolivia deberán tener registro e implementación de control de todas las direcciones MAC de los equipos de la entidad que estén conectados o dentro de la red.

DESIGNACIÓN DE PUNTOS A DESARROLLAR:

- Inclusión de términos y definiciones (todos)
- Agregar Light-Fi (Christian Urquiola - DGAC)
- Propuesta de Gobierno de TI. (André Mitsutake)
- Tipos de cableado y distancia óptima (buena práctica → anexo André Mitsutake)
- Etiquetado e infraestructura. (Wendy Sarmiento - Particular)
- Aislamiento de cableado horizontal en desuso (mencionar el estándar → Grover Medina - AJ).

ACUERDOS Y COMPROMISOS:

- Implementación de categorías A y B en infraestructura. (Todos: propuestas)
- Desarrollar respecto al uso de categorías 6A. (recomendaciones de cables blindados – buenas prácticas → Ángel Carani – Ministerio de Gobierno).
- Los integrantes de la mesa enviarán hasta el día jueves 18 de abril todos los aportes respecto a los puntos tratados y compromisos aceptados en los puntos a desarrollar.
- Revisión de registros MAC en la red de interoperabilidad (AGETIC).
- Próxima reunión del CTIC 22 de abril 16:00.