

<b>ACTA DE REUNIÓN</b>		
<b>Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia (CTIC-EPB)</b>		
<b>Grupo de Trabajo: SEGURIDAD</b>		
<b>Correlativo:</b> CTIC-SE-10/2019	<b>Fecha:</b> 17-07-2019	<b>Página:</b> 1/4
<b>Elaborado por:</b> Andre Mitsutake Cueto		

#### **ASISTENTES:**

De acuerdo a la lista adjunta.

#### **AGENDA DE TRABAJO:**

1. Revisión y comentarios la designación del punto de Desarrollo introducciones y subtítulos (Victor-INE; Shirley-SENASIR)
2. Análisis de propuestas y observaciones.
3. Aprobación de redacciones.
4. Designación de puntos para desarrollar.
5. Acuerdos para la siguiente reunión.

#### **DESARROLLO:**

[APROBADO]

##### **6.1.1 Seguridad en Infraestructura de Red**

La seguridad en la infraestructura de redes esta orientada a todo equipo de comunicación que tenga la función de asegurar los sistemas de información transportados a través de conexiones de redes dentro de la institución, entre instituciones o entre la institución y la población en general.

A seguir los lineamientos necesarios:

- Se debe contar con al menos un 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 de HUB (concentrador), para la mitigación de tormentas broadcast y otras vulnerabilidades o ataques (Andre).
- Se debe contar con al menos un dispositivo de capa 3 (switch-capa3, enrutador, etc.), para la administración 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.
- Se debe realizar la securización (hardening) de todo dispositivo implementado en la red de la institución.

<b>ACTA DE REUNIÓN</b>		
<b>Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia (CTIC-EPB)</b>		
<b>Grupo de Trabajo: SEGURIDAD</b>		
<b>Correlativo:</b> CTIC-SE-10/2019	<b>Fecha:</b> 17-07-2019	<b>Página:</b> 2/4
<b>Elaborado por:</b> Andre Mitsutake Cueto		

- Identificar y etiquetar de manera apropiada todo el equipamiento, medios de distribución y accesorios empleados en la implementación.<sup>1</sup>

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

- *Considerar la implementación de dispositivos de red redundantes para puntos de fallo único donde la disponibilidad sea un factor crítico.*<sup>2</sup>

- 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 tráfico 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 página web, e-mail, etc.

<sup>1</sup> Lineamiento y buenas prácticas para la implementación de un Centro de Procesamientos de Datos, CTIC-EPB, Pag,44

<sup>2</sup> Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público, CTIC-EPB, pag. 68

<b>ACTA DE REUNIÓN</b>		
<b>Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia (CTIC-EPB)</b>		
<b>Grupo de Trabajo: SEGURIDAD</b>		
<b>Correlativo:</b> CTIC-SE-10/2019	<b>Fecha:</b> 17-07-2019	<b>Página:</b> 3/4
<b>Elaborado por:</b> Andre Mitsutake Cueto		

- 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 SandBox, para disponer de un entorno aislado sin comprometer el resto de la infraestructura, de programas maliciosos.
- La implementación de soluciones Anti-SPAM para la mitigación de amenazas tales como phishing, spam y amenazas zombies-originadas.
- La implementación de dispositivos para salvaguardar la seguridad telemática siempre y cuando estas sean requeridas por los servicios y operaciones que cumple la institución

### **6.1.2 Seguridad en redes cableada**

Para garantizar la seguridad física de la red y la transferencia de datos a altas velocidades, es necesario asegurar las conexiones de red, compuesta por diferentes categorías de cables entre los nodos de un dispositivo a otro.

A continuación, se presenta lineamientos para la implementación de una red alambrada LAN<sup>3</sup>:

- *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.*

---

<sup>3</sup> Lineamientos y buenas prácticas para la implementación de un Centro de Procesamiento de Datos, Pag 48.

<b>ACTA DE REUNIÓN</b>		
<b>Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia (CTIC-EPB)</b>		
<b>Grupo de Trabajo: SEGURIDAD</b>		
<b>Correlativo:</b> CTIC-SE-10/2019	<b>Fecha:</b> 17-07-2019	<b>Página:</b> 4/4
<b>Elaborado por:</b> Andre Mitsutake Cueto		

<ul style="list-style-type: none"> <li>• <i>Identificar y/o etiquetar de forma apropiada todo el cableado entre los diferentes niveles, según la nomenclatura adoptada por la institución.</i></li> <li>• En relación a redes cableadas se recomienda las siguientes buenas practicas:</li> <li>• Emplear estándares de IEEE 802.3 para la implementación de medios físicos de comunicación.</li> <li>• Tener conexiones de redundancia en comunicaciones críticas dentro de la red local de la entidad.</li> <li>• Reducir al mínimo los puntos únicos de falla de la infraestructura de red.</li> <li>• 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.</li> <li>• 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).</li> <li>• Para nuevas implementaciones de infraestructura de redes y/o traslados de equipos, se recomienda verificar la certificación del cableado</li> </ul>
---

**DESIGNACIÓN DE PUNTOS A DESARROLLAR:**

<ul style="list-style-type: none"> <li>• Realizarlas referencias de todos los cites del lineamientos (ANDRE – AGETIC)</li> <li>• Averiguar tecnologías anti DoS a nivel red. (infraestructura recomendaciones) (Andre - AGETIC)</li> </ul>
--

**ACUERDOS Y COMPROMISOS:**

Revisión de redacción y subtítulos (TODOS)
--