1
08 2014 AÑO 1

SABER LIBRE

Revista digital sobre tecnología y conocimiento abierto

Soberanía tecnológica liberando el conocimiento

En este número:

COMUNIDAD SOFTWARE LIBRE BOLIVIA
http://www.softwarelibre.org.bo

Editorial

Como comunidad asumimos este reto con la colaboración de instituciones, profesionales y activistas amigos que hicieron de este un proyecto colectivo, siguiendo en si mismo la lógica del desarrollo del conocimiento y en sintonía con la forma en la que las y los bolivianos sabemos y hacemos las cosas: “en comunidad”. Creemos que en este encuentro en el marco del debate ideológico y académico podemos no solo reconocernos sino avanzar juntos compartiendo el conocimiento que como bien sabemos crece a medida que se comparte.

Esta iniciativa se inscribe en el escenario actual como un espacio de dialogo y expresión critica de temas poco escuchados y analizados en nuestro país; saberes, tecnologías, conocimientos, derechos y libertades acentúan y dan el marco para pensar nuestra sociedad como una sociedad de generación del conocimiento y no de reproducción de discursos y códigos culturales que lo limiten, apropien y mercantilicen.

Este primer numero coincide (no sin voluntad) con la contienda electoral que se vive en nuestro país, esperando aportar a dinamizar las discusiones y enriquecer los planteamientos de quienes en ella debaten con opiniones y argumentos serios. A su vez se enmarca en la campana “Yatiña Iyambae” o “Saber Sin dueño” que está dirigida a promover la liberación, el desarrollo y el acceso ir restricto al conocimiento y el uso de tecnologías libres.

En esencia, esta revista busca poner en contacto a quienes quieran debatir sobre el conocimiento libre en un camino que se inicia hoy y que esperamos podamos recorrer juntos por un largo tiempo.

El equipo de Saber Libre

Esta publicación fue realizada con:

Revista Saber Libre año 1, numero 1
Agosto 2014

Agradecimientos

- Centro de investigaciones de la Vicepresidencia del Estado Plurinacional

- Agencia para el Desarrollo de la Sociedad de la Información en Bolivia.

Comite Editorial

Tania Fatima Vega Gaspar
Mario Duran Chuquimia
Vladimir Castro Salas
Esteban Lima Torricos

Contactos
saberlibre@softwarelibre.org.bo

El software libre no puede ser el objetivo

Por: Ramón Ramón Sanchez
ramon@ramonramon.net

El software libre, al igual que las tecnologías, no puede ser el fin, son simples herramientas que nos proporcionan un mundo de oportunidades, de progreso, de avance,etc. o, mal usados, de ralentización y mantenimiento de la situación.

El software libre no puede ser el objetivoCon esta frase o afirmación, con la que comienzo este post, traslado mi visión de la situación actual del software libre en la Sociedad. Que además, es parte del prólogo que tuve el honor de escribir para el Quinto Informe anual de Valoración del software libre, publicado hace unos días, y que constata la actual realidad del software libre en Iberoamérica. Realmente este post, no es idéntico al prólogo, pues he quitado algunas estadísticas o datos del informe en sí, pero creo que recoge perfectamente lo que actualmente ocurre entorno al software libre en la sociedad iberoamericana.

El software libre es un concepto o término que se conoce en el ámbito de la tecnología, y por lo tanto, se relaciona con ésta misma desde hace décadas, aunque ha sido estos últimos años cuando se ha popularizado. Hablar de software libre hoy en día en Brasil, Ecuador o Venezuela, es hablar no de tecnología, sino de un modelo de país, un futuro de prosperidad y apropiación del conocimiento para su ciudadanía. Hablar de software libre en Extremadura o Andalucía es hablar de educación y e-inclusión, pues gracias al software libre existe en todos los colegios de estas dos regiones computadoras en todas las aulas, al igual que existen salas de alfabetización digital en todos los pueblos y zonas de riesgo de exclusión social. Aún así, en la mayoría de los casos, se sigue tratando al software libre como algo tecnológico, algo que tiene que ver con los informáticos, en lugar de con lo político, y por lo tanto, no se abordan como soluciones transversales sino como puntuales, o lo que es peor, como fin en lugar de como medio.

El software libre, y cada día son más los gobiernos y gobernantes que así lo consideran, se convierte en algo político, que no partidista, en una oportunidad de avanzar, de dejar de ser meros receptores y consumidores de tecnología para asumir el control de las mismas y generar riqueza, industria, empresa y capital humano formado.

Se trata de reivindicar, una vez más, que necesitamos valentía de nuestros gobernantes para acabar con la colonización tecnológica e igualmente, que como ciudadanía digital que somos, reivindiquemos a nuestros representantes que asuman su responsabilidad y no dejen en manos de transnacionales el control de nuestros datos, de nuestro conocimiento y de nuestro futuro.

Y es que, más importante que el software es el control de la tecnología y la defensa del conocimiento, poseer y compartir el Conocimiento nos hace avanzar, nos convierte en una ciudadanía más libre y con mayores posibilidades. El Conocimiento, en su sentido más amplio es la mayor riqueza que un pueblo puede tener, y por eso, es el bien más sagrado que debemos preservar, a la vez de compartir.

La tecnología no es neutral, no puede serlo, y el ejemplo más claro se plantea cuando son las multinacionales y no los estados los que poseen

los datos de su ciudadanía, los que deciden como afecta la tecnología al Estado y a la Sociedad en su conjunto. Cuando son las multinacionales las que poseen los datos, la información, e incluso deciden como deben realizarse los procesos y las comunicaciones, la tecnología pierde su sentido de herramienta El software libre no puede ser el objetivo y se convierte en el fin mismo, en el bien que toda empresa quiere poseer, expropiando a su verdadero poseedor, el Estado.

Usar software libre debe ser el vehículo que nos lleve hacia una verdadera soberanía tecnológica, que es el resultado de la libertad, entendida como no dominación de los estados frente a las corporaciones tecnológicas privadas y extranjeras.

Cada día que pasa más países lo entienden y se suman a la lucha por la libertad y la soberanía tecnológica, y no solo países, sino también regiones de todas las partes del planeta.

Es motivador ver lo claro que lo tienen en una importante cantidad de países de América Latina, con gobernantes como Brasil, más tras todos los últimos escándalos de espionaje a su presidenta, o Ecuador que ha decidido apostar por un modelo de crecimiento basado en la economía del bien común, mediante el proyecto FLOK Society: « Diseñando un cambio de matriz productiva hacia la sociedad del conocimiento libre, común y abierto ».

Es muy importante no caer en la tentación de los precios, hablamos de soberanía y de progreso, y para ello, necesitamos poseer el conocimiento y capacitar a nuestras generaciones en libertad y no en herramientas, que nuestros estados dejen de fomentar una determinada marca tecnológica, y lo que es aún más grave, usar los recursos públicos para formar exclusivamente en una tecnología.

Solo apostando por software libre y estándares abiertos obtendremos una Soberanía Tecnológica plena, y por lo tanto, tendremos el control total de nuestra tecnología, siendo dueños de nuestro presente y nuestro futuro.

Educación, Tablets y Aristóteles.

Por: Steve Fabián Conde Ordoñez.
fabianscs@gmail.com

Vivimos tiempos difíciles, con grandes retos en frente, como país, como humanidad. Los retos para las futuras generaciones serán aún mayores; la escasez de alimentos, la contaminación del aire, del agua, la destrucción de la naturaleza, la extinción de los animales, el calentamiento global, las guerras, los conflictos políticos internos y externos, luchas religiosas, las grandes diferencias sociales y económicas, etc. Estos son solo algunos de los problemas que ya enfrentamos y que muy probablemente se irán agravando.

Frente a este panorama no muy alentador se hace ineludible asumir nuestra responsabilidad de preparar a las presentes y futuras generaciones para enfrentar y tal vez resolver estos graves problemas. Debemos darles los instrumentos, herramientas y capacidades que les permitan superar estas adversidades, las cuales generaciones anteriores no han sido capaces de resolver, tampoco la presente, nosotros. Es entonces urgente darles a las nuevas generaciones el más valioso regalo, la educación, la mejor posible.

Una esperanza. La educación es y ha sido la más grande herramienta de progreso de la humanidad, ha ayudado a transformar y construir sociedades, la educación es la raíz del surgimiento y éxito de las civilizaciones, de la construcción de la ciencia y acumulación del conocimiento. Así como el gran pensamiento griego surgió influido en parte por avances egipcios y babilonios, el gran Aristóteles sólo pudo construir su monumental lógica en base a enseñanzas de su maestro Platón y éste a su vez aprendió de Sócrates. En base a la enseñanza y educación se construye, se avanza.

Se dice que el Aristóteles fue la primera persona en poseer una biblioteca personal y que esto le dio una ventaja decisiva sobre sus antecesores, “el conocimiento es poder” como diría Francis Bacon, me pregunto qué haría Aristóteles con la tecnología moderna, me pregunto qué pensaría si sabe que puede tener miles de libros en la palma de su mano, videos, contacto instantáneo con otras personas, cursos en línea, música, poesía, literatura, ciencia etc, etc. Hoy en día la tecnología ha abierto puertas inimaginables hace pocas décadas para acceder al conocimiento.

Conocimiento y tecnología. Es verdad, el avance tecnológico ha disminuido la brecha del conocimiento, por ejemplo antes de la era de las fotocopias era muy difícil acceder a los libros, especialmente por los altos costos, hoy en día no solo se puede acceder a las fotocopias mucho más económicas que los libros (los derechos de autor son otro tema), sino también a través de internet a miles y hasta millones de libros, videos, ensayos, artículos, foros de discusión, cursos online etc, etc.

“En la era de la información la ignorancia es una elección” reza una conocida frase de internet. Y es que hoy en día existe más información que nunca que además es accesible a más personas que todas las personas que tuvieron acceso al conocimiento en el curso de toda la historia de la humanidad juntas. Dentro de todas las posibilidades que nos brinda la tecnología podemos mencionar una en particular con mucho potencial, las tablets.

Tablets. Popularizadas por el visionario y gurú de la tecnología Steve Jobs, las tablets han ido conquistando el mundo, básicamente pantallas táctiles, que tienen hoy en día las mismas capacidades que sus primas lejanas (¿o antepasadas?), las grandes computadoras de escritorio.

Las tablets vienen en tamaños prácticos (de 7 y 10 pulgadas por ejemplo), cada vez más delgadas, ligeras,potentes, con gran independencia energética y capaces de realizar las más variadas tareas; conectarse a internet, realizar y recibir llamadas, editar textos (a todos los modelos de tablets se les puede acoplar ligeros teclados), realizar dibujos, reproducir videos, música y mi función favorita: se pueden usar como libros digitales cuya oferta no deja de crecer en internet en versiones gratuitas y pagadas, una biblioteca ilimitada en la palma de tus manos.

Vienen en una gran variedad de tamaños y precios, uno puede adquirir una Tablet de Samsung de 10 pulgadas por ejemplo en alrededor de 400 dólares (unos 2800 Bs.), existen versiones de 1000 dólares (7000 Bs.).

Estos son precios desde luego restrictivos, pero en el mercado existen soluciones mucho más económicas, el ejemplo más claro viene de la mano de la India y Datawind, el gobierno indio se propuso en dotar a 220 millones de estudiantes, la empresa británica Datawind ganó la licitación de resultado, las tablets llegan a un costo de 19 dólares (unos 132 Bs.) por estudiante (http://www.guioteca.com/cultura-india/la-tablet-mas-barata-del-mundo-esta-en-india-y-vale-us-19-dolares/), los cuales deberán pagar este costo pero además existe la posibilidad de pagar a plazos!.

El costo es subvencionado pero aun así el costo de la Tablet Aakash (que significa cielo en hindi) es de solamente 46 dólares (unos 320 Bs.), casi diez veces menos el costo de una Tablet Samsung cuyos modelos estándar cuestan alrededor de 400 dólares. Cabe decir que las tablets Aakash no tienen las mismas características que una Tablet Samsung desde luego, pero se han diseñado respondiendo a requerimientos del gobierno indio, y son capaces de responder con sus características a todos los requerimientos de los estudiantes con holgura, con su procesador Cortex a8 de 1 Ghz, 512 de Ram, wi fi (http://datawind.com/aakash/), se puede navegar por internet, reproducir videos, escuchar música, leer libros digitales con gran fluidez, aunque existen modelos con características superiores que aumentan el precio pero nunca pasando los 100 dólares.

Otra de las ventajas es que estas tablets (que son solo un ejemplo entre muchos), es desde luego que vienen con el sistema operativo Linux, software libre, gratuito y con muchas posibilidades de personalización, en cuanto al país, regiones o necesidades específicas para cada institución, su código abierto da muchas posibilidades a los desarrolladores, cosa que no permiten otros sistemas operativos como Windows 8.1. Además de la clara ventaja en el precio, una licencia estudiantil de Windows 8.1 cuesta alrededor de 560 Bs. (http://www.microsoftstore.com/store/mseea/es_ES/pdp/Windows-8.1-Pro---oferta-estudiantil/productID.288573500), aunque los precios varían de región en región, país a país, y de acuerdo al volumen de compra. En todo caso comprar este sistema operativo siempre significa un costo extra, el costo de Linux es 0.

Otro problema de comprar un sistema operativo de pago como Windows 8.1 es que hay que comprar además los programas adicionales como el conocido office. Cuyo costo para estudiantes esta en aproximadamente 750 Bolivianos (http://www.microsoftstore.com/store/mseea/es_ES/pdp/Office-365-Universitarios/productID.263156100), desde luego este precio puede variar como en el caso

ofertas gratuitas en Linux no solo una como es el caso de Office de Microsoft.

Posibilidades. Las posibilidades en el uso de las tablets son prácticamente ilimitadas, pero he aquí algunas de nuestras sugerencias, unas pocas.

Se podrá distribuir los textos estudiantiles en digital en vez de físicos, esto es una ventaja en cuanto a costos de distribución, producción, ecológicos, tiempos etc, etc, además que se podrán hacer las correcciones y actualizaciones a los textos de forma constante.
Acceso a bibliotecas digitales, vía internet y vía intranet.

Se podrán realizar conferencias, cursos y charlas para todos los estudiantes de Bolivia vía internet, no sólo de estudiantes sino también de profesores.

Se podrá usar software educativo especializado, diseñado en Bolivia y para la realidad boliviana.

Se podrán realizar encuestas en tiempo real a todos los estudiantes de Bolivia, de esta manera saber la opinión de estudiantes y profesores de todo el país en tiempo real.

Se podrán realizar evaluaciones tanto de estudiantes y profesores a nivel nacional, detectando fortalezas y debilidades. Imagínese hacer un examen de matemáticas a todos los alumnos de la promoción de Bolivia al mismo tiempo bajo supervisión de los profesores, se podrían reconocer talentos que de otro modo nunca se encontrarían.

Se podrá saber las fortalezas y debilidades de las distintas regiones tanto de profesores como alumnos pudiéndose tomar políticas educativas más eficientes.

Los estudiantes de todo el país y del área rural especialmente podrán acceder a contenidos a los que nunca pudieron acceder anteriormente ya sean libros, videos educativos u otros recursos de la red como cursos online.

Se podrá crear una red de cooperación e investigación estudiantil de Bolivia.

Se podrán lanzar convocatorias de lectura, escritura, ajedrez, matemáticas, etc, desde el ministerio de educación para promover el estudio en los jóvenes además de detectar estudiantes talentosos de todos los rincones del país.

Se podrán realizar votaciones en línea de estudiantes y profesores para conocer su posición de distintos temas en el ámbito educativo, también se podrán realizar debates sobre estos temas en foros educativos.

Se podrá tener un canal de radio, video o ambos en internet, para toda la comunidad educativa boliviana, con contenidos educativos y temas que le atañen a la comunidad educativa.

Dentro del aula los profesores podrán poner en pantalla de sus alumnos videos, imágenes o ejercicios, en cada una de las pantallas simultáneamente.

Los estudiantes podrán mandar la tarea por correo electrónico, el profesor podrá saber inmediatamente si se trata de un plagio de internet o una composición original del alumno.

Los estudiantes podrán profundizar en el tema o área que quieran con todos los recursos de la red de manera guiada y alentada.

El aprendizaje de los idiomas será más fácil, el Ministerio de ducación puede poner a disposición cursos extra para los alumnos en idiomas u otras áreas, los estudiantes que avancen podrían recibir incentivos, certificaciones académicas y otras cosas que fomenten el estudio y aprendizaje

de los alumnos. Así se mejoraría día a día el recurso humano de un país.

Se podrían lanzar campañas simultáneas a nivel nacional de diversas actividades como por ejemplo plantar árboles, aprender de la energía solar, sobre agricultura, etc. Se eliminaría toda la burocracia y la logística que este tipo de actividades conllevan, la convocatoria aparecería en la pantalla de los estudiantes, nadie sería discriminado de estas actividades.

El sistema. Estas son sólo algunas de las posibilidades que nos ofrece la tecnología, que permitirá un mejoramiento constante de la educación en Bolivia con la participación de toda la comunidad educativa.

Todos estos sistemas podrían centralizarse en servidores del ministerio de educación, que lance las convocatorias, albergue las librerías digitales, mande mensajes y material educativo, mantenga los contenidos y aportes de toda la comunidad educativa y del gobierno.

Con este intercambio de información bidireccional el Ministerio de Educación podría tener información precisa de las necesidades de la comunidad educativa para poder aplicar mejores políticas educativas, específicas a las necesidades de las regiones, la comunidad de estudiantes, profesores y padres podrían además coadyuvar permanentemente en el proceso de mejoramiento de la educación en Bolivia.

Conclusiones. El tiempo apremia para darles a nuestros hijos una educación que les permita afrontar los grandes retos que el mundo nos plantea hoy y mañana. La tecnología ofrece un sinfín de oportunidades para coadyuvar a este proceso (es una herramienta no lo es todo). Tenemos hoy al alcance de nuestra manos una gran oportunidad de dar un salto cualitativo y cuantitativo en la educación, tenemos las herramientas para echar las bases de un país sólido, productor y no consumidor de información y tecnología, es tiempo de poner todos nuestro máximo empeño para mejorar la educación, una educación libre, con tecnología libre, software libre y al alcance de todos.

Construyamos la Agenda digital para Bolivia

Por: Luis Rejas Alurralde
datamaxsp@gmail.com

Con motivo de la época electoral en la que nos encontramos en nuestro país, miembros del colectivo de ciudadanos denominado Más y Mejor Internet para Bolivia están impulsando los eventos para la creación de una agenda digital.

La Agenda Digital para Bolivia es una iniciativa mediante la cual se pretende propiciar un espacio de debate, por los propios ciudadanos y entre ellos, sobre el estado de la tecnología en nuestro país y generar una agenda conjunta de demandas ciudadanas al respecto, que les sirvan a los partidos políticos para que las hagan suyas, las analicen y las implementen dentro de sus programas electorales. Participarán en este debate especialistas, técnicos, activistas, académicos, emprendedores, y usuarios en general.

Para promover el debate permanente, se ha habilitado un sitio web (agendadigital.org.bo) en el que todos los ciudadanos están invitados a participar con sus planteamientos y propuestas. También se ha habilitado el grupo en Facebook (www.facebook.com/groups/AgendaDigitalBolivia/). En Twitter se está usando la cuenta @AgendaDigitalBO y la etiqueta #AgendaDigitalBO.

Se llevarán a cabo eventos presenciales de debate, inicialmente en la ciudades de La Paz, El Alto, Cochabamba y Santa Cruz. Hay otras ciudades que están solicitando incorporarse a esta rueda de eventos, por lo que hay más posibilidades de que encuentres un evento en el que puedas colaborar, participar y hacer oír tu voz.

En cada reunión se invitarán a especialistas en distintas áreas y se harán cargo de hacer un diagnóstico propio y promover el debate entre todos los asistentes.

El trabajo de sistematización de las conclusiones de estos debates, tanto en linea como presenciales, y su posterior conversión en el documento que constituirá la Agenda Digital, se ha optado por clasificar los diversos temas y problemática relacionados con la generación y uso de la tecnología en Bolivia en tres ejes principales; aunque no necesariamente limitados a ellos, ya que se pretende la mayor cobertura de las diversas voces ciudadanas:

* Infraestructura tecnológica y conectividad.
* Usos sociales de las TIC.
* Usos económicos: ecosistema para la innovación y el emprendimiento tecnológico.

Buscamos y necesitamos la participación y colaboración de la mayor cantidad posible de conciudadanos. Ayúdanos y ayúdate con esta iniciativa. Puedes colaborar de distintas maneras:

- Puedes apuntarte como voluntario para ayudar con la organización del evento presencial y su difusión en los medios periodísticos y las redes y para sistematizar la información obtenida tanto de los eventos como de la versión digital del debate mediante este formulario en linea: bit.ly/VoluntariosAgendaDigital

- Puedes participar del debate en linea en: agenciadigital.org.bo y los sitios en las redes sociales antes mencionadas.

Si tienes conocimiento avanzado de un área que te gustaría tocar podrías escribir un corto documento de dos a tres páginas y postular para ser expositor sobre este tema en el evento presencial escribiendo a datamaxsp@gmail.com

También estamos abiertos a cualquier otra idea que se te pueda ocurrir para conseguir el éxito de este proyecto.

Espionage & Cyber warfare (Espionaje y Ciber Guerra)

Por: Ivan Gutierrez Agramont,
Ph.D.c. in Secure Systems at UCB
ivan.guag@gmail.com

En estos últimos años cada día se habla más sobre la ciber guerra, pero esta guerra es muy diferente a todas las otras que el hombre se vio involucrado, ya que no hay una declaración, puede pasar sin saberlo y no necesariamente involucra a países, mas bien a diferentes grupos de personas de cualquier parte del mundo contra países, instituciones, entidades públicas y empresas públicas o privadas.

La ciber guerra tiene motivos económico, político y social y para muchas agencias de seguridad de países como Estados Unidos, Gran Bretaña, Unión Europea, Chile, Venezuela y Brasil entre los más importantes, es más peligroso que el terrorismo y narcotráfico. [1]

Los métodos de ataque son variados, pero los más importantes son:

Espionaje y seguridad nacional, para obtener información secreta, clasificada y en caso de empresas, obtener "Propiedad Intelectual", esto para obtener alguna ventaja, ya sea política, económica o militar.

Sabotaje, Servidores, equipos de comunicaciones y satélites, son los objetivos de este tipo de ataque, para causar cortes en servicios o comunicaciones. También los servicios básicos pueden ser atacados directa o indirectamente: (Energía eléctrica, agua, gas, gasolina o petroleo). [2]

Actualmente (desde el inicio del siglo 21), se vinieron haciendo este tipo de ataques con más frecuencia a entidades o empresas gubernamentales de todo el mundo, entre los más importantes están:

- OpUSA se llevo a cabo el 7 de Mayo de 2013, donde diferentes grupos de atacantes de todo el mundo atacaron mediante DDoS a 600 sitios web, el Deface de 73 sitios Web, la mayoría de los emails personales de funcionarios públicos fueron atacados, obteniendo sus contraseñas, los servidores de la policía de Hawai fueron bajados, un sitio de Microsoft fue deshabilitado, entre los ataques más importantes[9].

- A finales de 2011, Cert-In (Computer Emergency Response Team) India, reportó 13310 ataques a la infraestructura de ese país, desde las plantas nucleares hasta Telecomunicaciones y satélites espaciales[8].

- En Julio de 2011, la compañía Sur Coreana SK Communications fue atacada por un caballo de troya que obtuvo la información de todos sus empleados al rededor del mundo, información como nombre, dirección del domicilio, contraseñas de sistemas y correos electrónicos fueron comprometidos[10].

- En Junio de 2011 varios sitios de Chile, Perú, Colombia y Brasil fueron atacados por el grupo LulzSec, dando de baja a varios sitios web mediante ataques de DDoS[11].

- En Diciembre 2002, la empresa INTENSA realizó un ataque de control informático contra la empresa PDVSA en Venezuela, causando la paralización de la industria petrolera por varios días, el país se pudo recuperar de dicho ataque un año y medio después.[3][4]

Ahora, gracias a las filtraciones de Edward Snowden [12] sabemos que este tipo de guerra es llevada a cabo por estados, ya que Estados

Unidos realizo espionaje masivo a varios países en conjunto llevándolo a cabo con la implementación de puertas traseras (backdoors) o incluso con la entrega de datos por parte de empresas de internet como ser Microsoft, Facebook, Yahoo, Google y Twitter entre las más importantes [13].

Como hizo entonces la NSA para espiar a todos, no fue muy difícil, trabajo con las empresas de Internet (la mayoria de capitales y sedes estadunidenses) y añadió fallas explotables en sus productos[14] para así poder tomar control de la información y guardarla en sus propios servidores.

En caso de que alguna empresa no quiera colaborar, muchas fueron amedrentadas y finalmente cerradas (caso Lavabit)[15]

Entonces como afecta esto a los estados y a los ciudadanos?, de forma muy directa, ya que ninguna comunicación que se genere en servidores que NO sean propios y que NO pertenezcan a esas compañías es segura, la única forma es tener servicios propios seguros.

Entonces, cuales son las principales medidas que toman las agencias de ciber seguridad o los gobiernos (Estados)?, una de las principales es el uso de Tecnologías Libres y/o Abiertas como el Software Libre y el Sistema Operativo GNU/Linux, de esta forma garantizan independencia tecnológica y generan conocimiento sobre funcionamiento, protocolos de seguridad, algoritmos de cifrado, etc.

Porque entonces el Software Libre y de Código Abierto es más seguro, justamente por su propia naturaleza, la cual deja el código abierto a millones de programadores de todo el mundo, así como a agencias de seguridad, científicos e ingenieros del área de tecnología y computación. Una prueba clara es el Linux Security Modules, con todo su código liberado bajo una licencia libre.
Es en este sentido, que varios gobiernos en el mundo están apostando hacia este tipo de tecnologías, entre los principales están Brasil, Francia [6], Venezuela [7] Noruega, China y se espera que Bolivia también este en esta lista gracias a su Ley 164 de telecomunicaciones y TIC, la cual en su artículo 77 cito:

“Los órganos ejecutivo, legislativo, judicial y electoral, en todos sus niveles promoverán y priorizarán la utilización del software libre y estándares abiertos, en el marco de la soberanía y seguridad nacional. El órgano ejecutivo del nivel central del Estado elaborará el plan de implementación de software libre y estándares abiertos en coordinación con los demás órganos del Estado y entidades de la administración pública.”

Apelando así a este tipo de tecnologías por razones de Soberanía y Seguridad Nacional.

Referencias

[1] Dilanian, Ken."Cyber-attacks a bigger threat than Al Qaeda, officials say", Los Angeles Times, March 12, 2013
[2] Shiels, Maggie. (9 April 2009) “BBC: Spies 'infiltrate US power grid”. BBC News. Retrieved 8 November 2011.
[3] Ramon, Ramon (Noviembre de 2011) http://ramonramon.org/blog/2012/11/06/soberania-nacional-e-independencia-tecnologica/
[4] Jorge Hinestroza (Junio 2003) http://www.soberania.org/Articulos/articulo_333.htm
[5] http://www.nsa.gov/research/selinux/list.shtml
[6] http://www.techxav.com/2010/04/07/4-countries-that-strongly-support-open-source/
[7] http://softwarelibre.gob.ve/index.php?option=com_content&view=article&id=89&Itemid=82
[8] "Beware of the bugs: Can cyber attacks on India's critical infrastructure be thwarted?". BusinessToday. Retrieved January 2013.
[9] http://www.world-news.me/news/6gbTlWW56r?netloc=t_co&key

[10]"SK Hack by an Advanced Persistent Threat". Command Five Pty Ltd. Retrieved 24 September 2011.
[11]http://www.csmonitor.com/World/Americas/Latin-America-Monitor/2011/0623/LulzSec-Anonymous-show-Latin-America-unprepared-for-cyberwarfare
[12]
[13]http://elpais.com/elpais/2013/10/21/media/1382382712_305244.html
[14]http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
[15]http://news.cnet.com/8301-13578_3-57609722-38/lavabit-founder-says-he-fought-feds-to-protect-the-constitution/

Los derechos de los usuarios de telecomunicaciones vulnerados.

Por: Luis Rejas Alurralde
datamaxsp@gmail.com

La Constitución Política del Estado, en su artículo 20°, apartado I, dice que “toda persona tiene derecho al acceso universal y equitativo a los servicios básicos de agua potable, alcantarillado, electricidad, gas domiciliario, postal y telecomunicaciones”.

Para ello, este derecho se encuentra regulado, principalmente, en la Ley General de telecomunicaciones, tecnologías de información y comunicación.

Sin embargo, muchos usuarios ven vulnerados sus derechos.

Aquí tenemos dos de los artículos de la legislación de telecomunicaciones más vulnerados por las operadoras:

El artículo 54° de la mencionada ley, que dice: (Derechos de las usuarias y usuarios) Las usuarias o los usuarios de los servicios de telecomunicaciones y tecnologías de información y comunicación tienen derecho a acceder a información clara, precisa, cierta, completa, oportuna y gratuita acerca de los servicios de telecomunicaciones y tecnologías de información y comunicación, a ser proporcionada por los operadores o proveedores de los servicios.

El segundo es el artículo 120°, apartado IX, del reglamento general de esta ley, el Reglamento General de telecomunicaciones, tecnologías de información, que dice: sobre las prohibiciones y condiciones para la prestación del servicio: queda prohibido para el operador o proveedor migrar de una categoría tarifaria a otra, sin el consentimiento del usuario, salvo que la migración represente mayores beneficios y sean aceptadas por los usuarios.

Hemos observado, a lo largo de los últimos años, ante la pasividad y casi connivencia de la autoridad correspondiente, que estos preceptos son violados constantemente. Los ejemplos más comunes son:

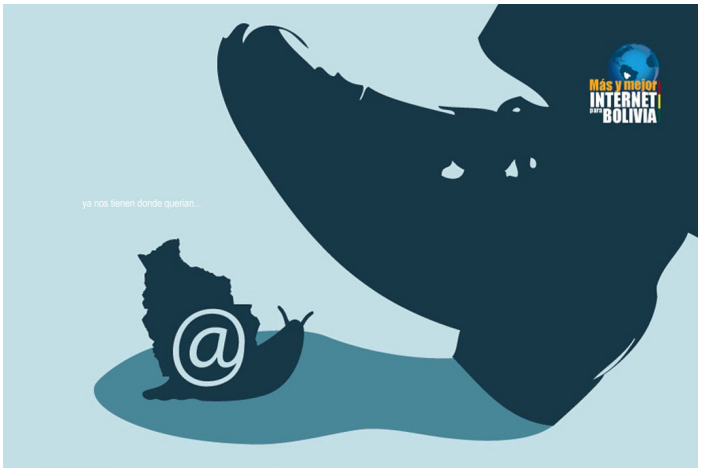
Que el usuario compre un paquete de Internet y, cuando se le acaban los MB o caduca la suscripción, la conexión permanece sin aviso de advertencia de que ahora le están cobrando en otro tramo tarifario, más caro y sin su consentimiento.

Otra situación detectada ha sido el caso del usuario que teniendo un plan por minutos, sin previo aviso ni consentimiento de este, le han cambiado a un plan por pulsaciones, que le acaba cuadruplicando el importe de su factura.

Lamentablemente las operadoras de telecomunicaciones en nuestro país están acostumbradas a vulnerar nuestros derechos, por el simple hecho de que los que reclaman por los mismos son un porcentaje muy pequeño, prácticamente inapreciable, o desde una perspectiva ejecutiva, no es necesario hacer modificaciones porque uno o dos clientes inconformes no afectan a los miles o millones de usuarios. En tal sentido las políticas, que obviamente benefician a las operadoras no se modifican.

Adoptemos entonces la cultura del reclamo y defendamos nuestros derechos y los de la comunidad hagamos evidente la necesidad de cambio, hagamos evidente este atropello contra

nuestros intereses y hagamos prevalecer lo que por derecho nos corresponde; Pues es la única forma de detener estos atropellos.



A continuación les dejo una lista de legislación pertinente a consultar, para quien desee profundizar:

Constitución Política del Estado.

Ley 2341 de Procedimiento Administrativo, de 23 de abril de 2002.

Reglamento de la Ley Nº 2341 de 23 /04/ 2002, de Procedimiento Administrativo, para el Sistema de Regulación Sectorial SIRESE, 15 de septiembre de 2003 (D.S. 27112).

Ley 164, General de telecomunicaciones, tecnologías de información y comunicación, de 8 de agosto de 2011.

Reglamento General a la Ley Nº 164, de 8 de agosto de 2011, General de telecomunicaciones, tecnologías de información, de 24 de octubre de 2012.

Ley 453, general de los derechos de las usuarias y los usuarios y de las consumidoras y los consumidores, de 6 de diciembre de 2013.

Otros de utilidad: Código Civil, Código de Comercio, Estatuto del Funcionario Público, Ley SAFCO.

Por último, sepan que si necesitan ayuda o consultar, me pueden encontrar en el grupo de discusión del colectivo Más y Mejor Internet para Bolivia:

https://www.facebook.com/groups/adslbolivia/

en mi blog:

http://dolordecabezacontigo.blogspot.com/

o en Twitter: @LuixSP

Educación de calidad para todos

Por: Jorge Teran Pomier
Universidad Mayor de San Andrés
teranj@acm.org

En la actualidad tener educación especializada es cada vez más sencillo gracias a los medios tecnológicos en el que se destaca Internet. Existen una serie de cursos en línea gratuitos de las universidades más prestigiosas del mundo. En línea quiere decir precisamente accesibles por medio de internet. En este articulo haremos una breve descripción de diferentes tipos de cursos y dejaremos los enlaces para que todos puedan inscribirse y participar de los mismos.

Podríamos dividir la educación en línea en tres grupos principales:

- AudioVisuales por medio de canales educativos como ser Youtube, Vimeo, entre otros.
- Los cursos denominados Open courseware (OCW)
- Los cursos masivos en línea (MOOC)

AudioVisuales por medio de canales educativos

Muchas universidades tales como Mit, Stanford, universidades españolas, etc., han subido cursos completos en vídeo, los que se pueden acceder libremente por Youtube y otros. Los cursos de las instituciones académicas se acceden buscando lo que se denominan canales educativos.

En algunos otros sitios se denominan simplemente categorías.

Las diferencia de los canales educativos con solamente diferenciarlos por categorías es que las instituciones educativas disponen de un espacio especifico para su institución. Esto hace que uno pueda tomar los cursos de una institución especifica.

Open Course Ware (OCW)

Es la publicación de materiales educativos como "contenidos abiertos". Generalmente son los docentes los que ceden algunos de sus derechos de propiedad intelectual, como ser la distribución, reproducción, comunicación pública o generación de obra derivada. No solo son contenidos de acceso libre como los canales educativos de Youtube sino que además se puede reutilizar libremente respetando la cita del autor original. Generalmente corresponden a asignaturas de la educación superior universitaria, tanto de grado como de postgrado.

Este concepto fue iniciado por el Instituto Tecnológico de Massachusetts (MIT) y hoy en día muchas universidades proporcionan este tipo de cursos. La estructura depende de la institución educativa o del que estructuro-creo. Usualmente consisten de los vídeos de los cursos y los materiales proporcionados por el docente a los estudiantes.
Una lista larga de estos cursos pueden verse en http://es.wikipedia.org/wiki/OpenCourseWare.

Existen cursos de universidades de todo el mundo, así como de varias universidades latinoamericanas, que tienen materiales en español.

Cursos masivos en línea (MOOC)

MOOC viene de su acrónimo en ingles "massive open online course", que significa cursos abiertos y masivos en línea. Se ofrecen cursos de pregrado y postgrado en forma gratuita y

y con gran calidad.

Esta iniciativa se inicio en la universidad de Utha el 2007. El primer hito se dio con un curso de la Universidad de Stanford que matriculo 160,000 estudiantes.

Entre las plataformas más reconocidas podemos mencionar:

- Udacity de la Universidad de Stanford

- Coursera conformado por Yale, Princeton, Michigan, Penn, UNAM, Universitad Autonoma de Barcelona, Instituto Tecnológico de Monterrey

- Edx del Instituto tecnológico de Massachusetts

- Miriada X conformado por la universidades Miríada X Universidad de Huelva,Universidad de Puerto Rico, Universidad Carlos III, Universidad Tecnológica de Pereira,Universidad CEU San Pablo, Universidad CEU Cardenal Herrera, Universitat de Girona, Universidad Politécnica de Madrid, Universidad de Zaragoza, Universidad Católica de Murcia, Universidad de Salamanca, Universidad de Alcalá, Universidad Católica Santo Toribio de Mogrovejo, Universitat Pompeu Fabra, Universidad Politécnica de Cartagena, Universidad San Martín de Porres, Universidad de Ibagué, Universidad Blas Pascal, National University College, Universidad de Alicante, Universidad Politécnica de Valencia, Universidad Europea, Universidad Abierta Para Adultos, Universidad, Complutense de Madrid, Universidad de Cantabria, Universidad de Murcia, Universidad, Nacional de Educación a Distancia (UNED), Universidad Rey Juan Carlos, Corporación, Universitaria Minuto de Dios (Uniminuto), Universidad Autónoma de Occidente (UAO)

¿Cuál es la diferencia entre estos cursos y los tutoriales o blogs publicados en en el internet?

Bueno esto son cursos auspiciados y respaldados por centros de formación, generalmente universidades, lo que garantiza la calidad puesto que expone el prestigio de la institución.

Con relación a los aspectos de licencias y condiciones para reutilizar el material cada institución define la misma. Generalmente se puede reutilizar sin pedir ninguna autorización para fines educativos.

Algo que puede preocupar a muchos es la certificación. La mayoría de estos cursos no ofrecen un certificado. Por ejemplo en Cursera no se dan certificados, sin embargo algunos docentes dan un certificado a sus estudiantes.

Entre los retos del los cursos masivos, aún se deben resolver es la relación docente estudiante, dado que en muchos casos puede desaparecer.

En los curso OCW y los vídeos en línea, no hay relacion docente -estudiante, es solo el interés ya sea de un docente o estudiante de revisar un curso de una universidad.

Seguridad Informática en la Seguridad de Estado

Por: Wilfredo Mendoza Murillo
Postgrado en Informática -UMSA
wmendozam@gmail.com

Abstract

El tema de la Seguridad de Estado, desde tiempos remotos, es un tema que no se ha dejado de lado en ningún momento y, cuando hablamos de Seguridad Nacional o Estado fácilmente nos viene a la mente un sin número de armas, una imagen de un agresor físico, una idea de vulnerabilidad, pero cuando nos preguntamos que estamos protegiendo y cómo lo hacemos, posiblemente se nos viene a la mente muchos elementos y entre ellos la vida humana y el cómo posiblemente nuestra mente se quede en blanco por un momento y piense en armamento pesado.

En la actualidad la Seguridad de Estado, en muchos de los países desarrollados y en desarrollo, se ha convertido en un foco de análisis, debido al avance tecnológico, avance informático que está en todas partes e ingreso a todos los campos, el avance tecnológico hace que la informática vaya de la mano con la misión y visión de cada una de las instituciones que pertenecen al Estado y mucho más con la instituciones encargadas de las Seguridad de Estado, pero cuan seguros estamos de que la informática que manejamos es segura.

La Seguridad de la Informática debe estar presente a la hora de implementar cualquier proceso de automatización que involucre la Seguridad de Estado. Ya sean procesos complicados que involucren, comercio electrónico, gobierno electrónico o simplemente la transferencia o envío de un documento digital, o cálculos de los sueldos y salarios, como el control de las fronteras de un Estado.

Índice de Términos—Seguridad, Informática, Estado, Información, Centro de Cómputo

[i] Introducción.

En un principio haremos un enfoque de lo que involucra Seguridad de Estado, debido a que dentro de un Estado se maneja un conglomerado de sistemas de seguridad, sin embargo en la actualidad en la mayoría de los Estados, el análisis de la Seguridad se va centrando en los avances Tecnológicos, el uso de medios electrónicos para el tratamiento de los Datos a niveles de decisión, que en su momento permiten conocer la situación interna de un Estado, respecto a una región, un continente o mundial.

El uso de las ISO respecto a la seguridad de Información es un apoyo muy importante que viene a complementar el tema de Seguridad Informática.

[ii] Seguridad del Estado.

"Barry Buzan en su estudio People, Status and Fear dice que la seguridad debe incluir aspectos económicos, políticos, sociales, de medio ambiente, lo mismo que militares, y que a su vez está definida en términos internacionales más amplios. Su concepto de seguridad es más amplio y permite una apreciación de los elementos más allá de las cuestiones militares, que encierra la seguridad en un complejo sistema internacional"[1], en efecto un estado debe preocuparse no solamente de la seguridad humana, del territorio que ocupa, la economía que mantiene, hoy por hoy la información generada por un estado.

Todas las leyes de los Estados fueron adaptándose con el pasar de los años, en el caso del Estado Plurinacional de Bolivia, una de las atribuciones del Presidente es el de Preservar la seguridad y la defensa del Estado.

Pero institucionalmente el artículo referido a la Seguridad del Estado "Artículo 244. Las Fuerzas Armadas tienen por misión fundamental defender y conservar la independencia, seguridad y estabilidad del Estado, su honor y la soberanía del país; asegurar el imperio de la Constitución, garantizar la estabilidad del Gobierno legalmente constituido, y participar en el desarrollo integral del país" [2]. Que también involucra la policía nacional en el ámbito del Local.

Pero jurídicamente los términos de Soberanía y Seguridad Nacional y van repitiendo, tal es el caso de la Ley 164 en el caso Boliviano, Ley General de Telecomunicaciones y Tecnologías de Información y Comunicación, en el artículo 77. Debido a que el avance tecnológico obliga a los estados a no quedarse sin tomar decisiones que permitan el desarrollo de un Estado de acuerdo normativas Internacionales, en su beneficio.

[iii] Seguridad Informática.

Si tomamos en cuenta la evolución la evolución de las computadoras como herramienta que apoya a la Informática, en los años 60' "la informática estaba en manos de muy pocos fabricantes e imperaba la filosofía del servicio integral: cada fabricante lo proporcionaba todo (ordenadores, cables, periféricos, sistema operativo y software). Por tanto, cuando una empresa se quería informatizar, elegía una marca y quedaba vinculada a la misma para toda la vida" [3], en los 70' este paradigma cambió totalmente, "sobre todo a causa de tres acontecimientos:

- La propuesta del protocolo Ethernet para redes locales.

- La aparición del sistema operativo Unix, que no estaba vinculado a ninguna marca comercial, compatible con todas las plataformas de hardware existentes.

- La invención de los protocolos TCP/IP, embrión de la actual Internet." [4]

Entonces una institución sea del Estado o privado podía adquirir distintos tipos de hardware para armar su centro de cómputo, y el control de la seguridad ya no estaba en manos de los proveedores.

La "seguridad informática como una disciplina del conocimiento donde se busca cerrar la brecha de los eventos inesperados que puedan comprometer los activos de una organización y así contar con estrategias para avanzar ante cualquier eventualidad" [5],

[iv] Pilares de la Segurida Informática.

No se debe confundir la Seguridad de la Información[6] con la Seguridad Informática, debido a que se entiende por Seguridad Informática al conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de Información.

Confidencialidad.- la informaciónpuede ser accedida, únicamente por las personas que tiene autorización parahacerlo.

Integridad: La información no ha sido borrada, copiada o alterada, no solo en su trayecto, sino también en su origen.

Disponibilidad: Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen.

Estos pilares son de especial cuidado ya que si no uno de ellos no se cumple en la

configuración de la Seguridad de la Informática de las instituciones públicas de un estado, no se cumplen con las normas ISO, por lo tanto estaremos a expensas de los nuevos intrusos informáticos en busca de cometer algún delito informático.

[v] ¿Qué debemos proteger?

Al encontrarse la información en medios de procesamiento Informático, estos dispositivos electrónicos y los accesos a los mismos desde cualquier punto de riesgo nos deben llevar reflexionar sobre lo que queremos proteger.

Sin embargo en la actualidad tenemos herramientas como son la familia de la ISO 27000, que nos ayudan a determinar los activos informáticos, que en la mayoría de los casos se trata de todo tipo de dispositivos que nos permiten el recojo, almacenamiento, la administración de datos y la continuidad en la producción y explotación de dichos datos. Lo que involucra, todo tipo de data center, medios de comunicación interna, externa, incluyendo dispositivos que garanticen el fluido eléctrico, incluyendo a las personas encargadas de estos procesos.

Las instituciones del estado, a través del área de Auditoría Informática, debe aplicar la Gestión de Activos de la Información [7], con la finalidad de conocer lo que debe proteger, y buscar asegurar estos equipos contra delitos informáticos ante las empresas de seguros.

[vi] ¿De quien debemos proteger?.

La protección Seguridad Informática, intenta proteger cuatro elementos, como son Hardware, Software, Datos y Elementos consumibles, estos datos tiene un grado de confidencialidad, estos datos que pueden ser económicos, demográficos u de otra categoría, debemos protegernos de todo riesgo conocido.

[vii] Mecanismos de Seguridad.

Un mecanismo de seguridad es una técnica o herramienta que se utiliza para fortalecer la confidencialidad, la integridad y/o la disponibilidad de un sistema informático.

Estos mecanismos deben tomarse de acuerdo al tipo de sistema, la función que cumple y los factores de riesgo que lo pueden amenazar.
Clasificación según su función:

Preventivos: Actúan antes de que un hecho ocurra y su función es detener agentes no deseados.

Detectivos: Actúan antes de que un hecho ocurra y su función es revelar la presencia de agentes no deseados en algún componente del sistema. Se caracterizan por enviar un aviso y registrar la incidencia.

Correctivos: Actúan luego de ocurrido el hecho y su función es corregir la consecuencias.

[viii] Riesgo.

“En los comienzos de la informática, había un rechazo al uso de las computadoras (y del software) para el control de procesos críticos de seguridad como por ejemplo reactores nucleares, control de vuelos de aviones, sistemas de armamento y grandes procesos industriales”.[8], Hoy en día, se emplean regularmente hardware y software para el control de sistemas de seguridad crítica.

Dentro de la Seguridad del Estado, habría que estar alerta para identificar riesgos, Una vez que se han identificado y analizado los riesgos, se pueden especificar los requisitos relacionados con la seguridad para esta informática utilizada, lo que significa que, la especificación puede contener una lista de eventos no deseables y las respuestas del sistema de Seguridad a estos eventos. Y si estos procesos están automatizados, el papel del software en la gestión de eventos no deseados es entonces apropiado.

Los riesgos ambientales físicos deben ser una preocupación constante, tales como, factores externos, lluvias, inundaciones, terremotos, tormentas, rayos humedad, calor entre otros.

Riesgos Tecnológicos como fallas en el funcionamiento de hardware y software, en el aire acondicionado, el fluido eléctrico, ataque por virus informático.

Riesgo Humano donde está presente el hurto, adulteración, fraude, modificación revelación, pérdida, sabotaje, vandalismo, hackers, crackers, robo de contraseñas, falsificación y otras.

[ix] Interoperabilidad.

Otro tema que surge cuando un Estado desea tener relaciones tanto al interior como al exterior, de sus fronteras, tiene que concentrarse en la interoperalibilidad. “Se entiende por interoperabilidad la habilidad de organizaciones y sistemas dispares y diversos para interactuar con objetivos consensuados y comunes y con la finalidad de obtener beneficios mutuos.

La interacción implica que las organizaciones involucradas compartan información y conocimiento a través de sus procesos de negocio, mediante el intercambio de datos entre sus respectivos sistemas de tecnología de la información y las comunicaciones”. [9].

Pero la interoperabilidad tiene varias dimensiones. Generalmente, se suele hacer referencia a:

- La interoperabilidad técnica: Se refiere a aquellas cuestiones técnicas que garantizan que los componentes tecnológicos de los sistemas de información de las entidades participantes estén preparados para colaborar todos juntos.

Permite, por tanto, proporcionar mecanismos comunes de transferencia de los datos y de invocación de funciones, transparentes al sustrato de redes y sistemas informáticos existentes. Entre otras cuestiones, se refiere a interfaces, servicios de interconexión, integración de datos, middleware, presentación e intercambio de datos, accesibilidad o servicios de seguridad.

- La interoperabilidad semántica: Se ocupa del significado en el uso de los datos y la información y, en concreto, garantiza que el significado preciso de la información intercambiada pueda ser entendido por cualquier aplicación.

- La interoperabilidad organizativa: Aborda la definición de los objetivos de los procesos servicios de las organizaciones implicadas en la prestación de servicios telemáticos o de iniciativas de cooperación e integración de back offices. La interoperabilidad organizativa asegura la coordinación y el alineamiento de los procedimientos administrativos que intervienen en la provisión de los servicios de Gobierno electrónico. 28

[x] Avances.

Como en todo el mundo, vemos un ejemplo en España, El objetivo principal del Amper.LAB “es procurar la infraestructura técnica y recursos necesarios para:

Integrar las soluciones networkenabled (NEC) en un centro de experimentación con una arquitectura basada en servicios (SOA).

Desplegar tanto nuevos sistemas como sistemas anteriores permitiendo su interoperabilidad, así como interoperar con sistemas de terceros.

Proporcionar capacitad de interconexión con centros de experimentación del Ministerio de Defensa.

Disponer de una Networking and Information Infrastructure sobre los sistemas de

telecomunicaciones en servicio (RBA/CNR, RETUME) y futuros (SDR, RTIP, WiMax, etc.) de forma que se pueda medir la eficacia de los sistemas de información en un entorno real.

Facilitar la experimentación en nuevos conceptos y capacidades militares permitiendo la incorporación de nuevos avances tecnológicos y su desarrollo.

Proporcionar una herramienta que permita la elaboración de CONOPS a los Estados Mayores."[10]

La tecnología ayuda a mejorar las soluciones estratégicas para la Seguridad de Estado.

[xi] Mecanismos de Seguridad.

Son necesarios los mecanismos de seguridad toda vez que se empiezan a encontrar vulnerabilidades, para mitigar las amenazas, un proceso del que se nutre la informática es:

Intercambio de información: Cuando se intercambia información con un ordenador remoto, esa información circula por una serie de sistemas intermedios que son desconocidos a priori (excepto en ámbitos muy específicos). Además, no sólo no se sabe cuáles serán estos sistemas intermedios, sino que además no se dispone de ningún control sobre ellos o sobre lo que puedan hacer con nuestros datos al pasar por ellos.[11]

Instalación de software dañino involuntariamente: Otra posibilidad que no se debe descartar es que se instale software en un ordenador sin conocimiento del usuario o administrador [12]. Los que involucran virus o troyanos, por descarga de software de la red, sin conocimiento del usuario, al igual que los adjuntos en los correos electrónicos, o explotación de carpetas compartidas en la red.

Protección ante accesos no autorizados: Cuando se ofrecen servicios o información en una red para sus usuarios legítimos, al mismo tiempo se abre la puerta a posibles intrusos en estos sistemas.

Protegerse de esta posibilidad implica tener un especial cuidado con todo el software empleado, desde el sistema operativo hasta la última de las aplicaciones instalada, y cuidar en gran medida su configuración [13]. En efecto son las vulnerabilidades encontradas por intrusos de la red, con fines no muy amigables.

En tal sentido se hace necesario de

[xii] Software Libre y la Seguridad Informática.

"En general se entiende como software libre aquel programa o conjunto de ellos de los que el usuario puede disponer del código fuente, sin restricciones, y el cual puede modificar y redistribuir también sin restricciones"[14] http://www.debian.org/social_contract#guidelines, Entre las licencias más utilizadas para este tipo de software cabe destacar la licencia GNU GPL http://www.gnu.org/copyleft/gpl.html y la licencia BSD (http://www.debian.org/misc/bsd.license)., al disponer del código fuente, surgen algunas acciones de control de Seguridad Informática, como son:

El análisis del código fuente por terceros, ajenas al autor en busca de fallos de diseño o implementación.

Las modificaciones, que se pueda hacer sobre el código fuente, deben reflejar mejoras, como nuevas funcionalidades o parches que corrijan errores anteriores.

Dado que las características del Software Libre hace que no se pueda incrementar costes.

Se puede adaptar a las necesidades de la entidad que la utiliza teniendo el control de las funcionalidades eliminadas.

Pero también otorgan cierta protección a los usuarios, con algunos mecanismos como:

La posibilidad de una auditoría al código fuente utilizado.

La posibilidad de que los parches se los pueda realizar por un número de personas y no por un solo fabricante.

La independencia que existe entre el software y el que lo desarrollo, permite que los usuarios de éste software, en caso de pérdida de soporte, puedan realizar el mantenimiento ellos mismos o contratar a terceras personas.

[xiii] Desventajas del Software ante la Seguridad Informática.

Tanto el Software Propietario, como el Software Libre tienen algunas desventajas frente a lo que requiere la Seguridad Informática, que en su momento puede volcarse en contra de la Seguridad de Estado que viene a ser el usuario final, en el software propietario:

-Existe la posibilidad de que existan funcionalidades no deseadas en dicho software.

-Desconocimiento del código por parte del usuario.

-Necesidad de confiar plenamente en el desarrollador.

-Dependencia de una tercera entidad, ya que el fabricante del producto es el único que ofrece nuevas versiones.

En lo que se refiere al software libre, se indica que:

La posibilidad de generar más fácilmente los troyanos, debido a que el código fuente también puede ser modificado maliciosamente.

El método de la generación del código fuente, que se lo realiza en distintos lugares, y que por alguna razón falten piezas clave, como la documentación.

Al no tener un respaldo directo, la evolución futura de los componentes software no está asegurada o se hace demasiado despacio[15]

[xiv] El Modelo de Métodos Formales.

Dentro de la Ingeniería del Software, para el desarrollo de Software, algunas organizaciones deben seguir ciertos modelos con la finalidad de desarrolla un software de mucha seguridad, “Los métodos formales permiten que un ingeniero de software especifique, desarrolle y verifique un sistema basado en computadora aplicando una notación rigurosa y matemática”[16], lo que se elimina con este modelo, son la ambigüedad, lo incompleto y la inconsistencia, se descubren y se corrigen más fácilmente mediante la aplicación del análisis matemático.

Sin embargo, se ha hablado de una gran preocupación sobre su aplicabilidad en un entorno de gestión:

1. El desarrollo de modelos formales actualmente es bastante caro y lleva mucho tiempo.

2. Se requiere un estudio detallado porque pocos responsables del desarrollo de software tienen los antecedentes necesarios para aplicar métodos formales.

3. Es difícil utilizar los modelos como un mecanismo de comunicación con clientes que no tienen muchos conocimientos técnicos.

No obstante es posible que el enfoque a través de métodos formales tenga más partidarios entre los desarrolladores del software que deben construir software de mucha seguridad (por ejemplo: los desarrolladores de aviónica y dispositivos médicos), y entre los

desarrolladores que pasan grandes penurias económicas al aparecer errores de software [17].

[xv] La integridad del Software.

"En esta época de «hackers» y firewalls», la integridad del software ha llegado a tener mucha importancia. Este atributo mide la capacidad de un sistema para resistir ataques (tanto accidentales como intencionados) contra su seguridad. El ataque se puede realizar en cualquiera de los tres componentes del software: programas, datos y documentos. Para medir la integridad, se tienen que definir dos atributos adicionales: amenaza y seguridad.

Amenaza es la probabilidad (que se puede estimar o deducir de la evidencia empírica) de que un ataque de un tipo determinado ocurra en un tiempo determinado. La seguridad es la probabilidad (que se puede estimar o deducir de la evidencia empírica) de que se pueda repeler el ataque de un tipo determinado. La integridad del sistema se puede definir como:

integridad = SUM(1 - amenaza) x (1 - seguridad)]
donde se suman la amenaza y la seguridad para cada tipo de ataque.

[xvi] El papel de las ISO en Seguridad Informática.

El uso de Estándares dentro de la Seguridad de la Información, se viene trabajando desde hace bastante tiempo, El estándar ISO 9126 ha sido desarrollado en un intento de identificar los atributos clave de calidad pira el software. El estándar identifica seis atributos clave de calidad:

Funcionalidad. El grado en que el software satisface las necesidades indicadas por los siguientes subatributos: idoneidad, corrección, interoperatividad, conformidad y seguridad.

Confiabilidad. Cantidad de tiempo que el software está disponible para su uso. Está referido por los siguientes subatributos: madurez, tolerancia a fallos y facilidad de recuperación.

Usabilidad. Grado en que el software es fácil de usar. Viene reflejado por los siguientes subatributos: facilidad de comprensión, facilidad de aprendizaje y operatividad.

Eficiencia. Grado en que el software hace Óptimo el uso de los recursos del sistema. Está indicado por los siguientes subatributos: tiempo de uso y recursos utilizados.

Facilidad de mantenimiento. La facilidad con que una modificación puede ser realizada. Está indicada por los siguientes subatributos: facilidad de análisis, facilidad de cambio, estabilidad y facilidad de prueba.

Portabilidad. La facilidad con que el software puede ser llevado de un entorno a otro. Está referido por los siguientes de la Ingeniería del Software, para el desarrollo de Software, algunas organizaciones deben seguir.

[xvii] Seguridad Informática y la encriptación.

En la actualidad donde el flujo de información se lleva a cabo desde un domicilio particular a través de Internet, por medio inalámbricos de transmisión de datos, es hora de ponernos a pensar que está pasando ahí afuera, porque los intrusos no necesitan ingresar a su domicilio, las típicas intrusiones ahora están en:

Un intruso monitoriza el tráfico de una línea de transmisión y recoge la información confidencial que genera un usuario.

Un intruso podría entrar en un sistema distribuido, acceder a la base de datos y cambiar la información de la misma.

Un intruso podría leer una transacción que pasa por alguna línea de transmisión y alterar los datos dentro de ella en beneficio propio.

Un ex empleado contrariado de una compañía envía un programa al sistema distribuido de la compañía monopolizando el tiempo del procesador del sistema, pasando gradualmente de servidor a servidor hasta que el sistema queda exhausto y acaba parándose.

Un empleado contrariado de una compañía envía un programa a un sistema distribuido el cual borra los archivos importantes del sistema.[18]

Como se puede notar, estamos frente a varios tipos de intrusión, por este motivo existen protocolos de comunicación, protocolos con o sin algún tipo de seguridad, dentro de las técnicas más utilizadas entre la comunicación de dos fuentes, la encriptación de datos basados en modelos matemáticos, donde el proceso realizado es:

1. La computadora emisora transforma el texto en alguna forma ilegible; este proceso se conoce como encriptación.

2. Los datos encriptados entonces se envían a través de líneas de transmisión insegura.

3. La computadora receptora procesa el texto encriptado y lo transforma a su forma original. Este proceso se conoce como desencriptación. [19]

En Internet podemos decir indicar los métodos sobre envío y recepción de contraseñas.

El Mando de Acceso de contraseña: La manera

más intuitiva de realizar el mando de acceso es pedir una contraseña. Cuando un cliente desea conectar a un servidor, ellos pueden proceder como sigue.

1. el cliente envía una demanda de acceso primero al servidor.

2. el servidor reconoce y envía una demanda de la contraseña al cliente.

3. el cliente envía su contraseña al servidor.

4. el servidor verifica la exactitud de la contraseña y proporciona o niega el acceso al cliente.[20]

Las Contraseñas de UNIX: Aquí, el cliente es un usuario (o un proceso de UNIX cuyo se asocian los permisos al usuario) y el servidor es un puesto de trabajo. Aquí el servidor debe guardar una base de datos de “encriptación” (a través de una función sentido único) las contraseñas. El encriptación sentido único es intencionalmente lento para reducir la velocidad los ataques de mando de acceso.

Mando de Acceso básico en HTTP: Otro ejemplo de mando de acceso de contraseña que se toma de RFC2617, se usa en el protocolo de HTTP. Aquí el cliente está un navegador que desea tener el acceso a un documento protegido llamó el identificador del recurso uniforme (URI) de un sitio de Web.

El Mando de Acceso de PAPILLA en PPP :Un ejemplo similar es uno de los dos protocolos de mando de acceso proporcionado en el Punto para Apuntar el Protocolo (PPP) qué permite la conexión remota de una máquina a una red.

La Comunicación inalámbrica: Dos casos para ser nombrados.

- La Red de GSM GSM (las comunicaciones de SystemforMobile Globales) es una norma desarrollada por ETSI para las comunicaciones del mobilewireless. Incluye las normas de seguridad. Los objetivos de seguridad son bastante bajos en el sentido que ellos sólo previenen los ataques contra el cauce de la radio entre el término y una base fija.

-La Red de Bluetooth Las redes de Bluetooth son otros ejemplos buenos de infraestructura de seguridad sólo basados en la criptografía convencional. Nosotros perfilamos brevemente cómo funciona basado en el Bluetooth versión 1.2.

[18] Conclusiones.

En Seguridad Informática en la Seguridad de Estado, nada está dicho, debido a que la Tecnología sobre la que se basa la informática de un Estado, cada día es más sorprendente, leguajes de programación, tipos de almacenamiento masivo de información, donde las redes sociales se adueñaron de los primeros lugares de los sitios más visitados, manejo de frameworks, donde se empieza a fundamentar el uso de software privativo o software libre, más banda ancha para el intercambio de comunicación, interoperabilidad interna y externa, sin embargo aplicar normas internacionales, adecuadas al Estado, que involucran planes de contingencia, planes de continuidad, son imprescindibles, así como aprender a comprender los avances tecnológicos y así aprovechar la convergencia tecnológica en beneficio del Seguridad de Estado.

Referencias.

[1] María Elena Romero, "La seguridad nacional japonesa y las cuestiones económicas", revista mexicana de estudios sobre la Cuenca del Pacífico / Volumen 3 • Número 6 / Julio • Diciembre 2003 / p.p 4.

[2] Constitucion Politica del Estado Plurinacional de Bolivia, pp.40

[3] José María Barceló Ordinas, Jordi Íñigo Griera, Ramón Martí Escalé, EnricPeig Olivé, Xavier PerramonTornil, XP04/90786/00020, "Redes de computadores" UniversitatOberta de Catalunya Pag. 31.

[4] W.-K. Chen, Linear Networks and Systems (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.

[5] Jeimy J. Cano, "Inseguridad informática un concepto dual en seguridad informática" Universidad de los Andes, dorde se concentra en los temas de Seguridad Informática, Computación Forense y Evidencia Digital, Universidad de los Andes, pag. 46.

[6] Erick A. Lamilla Rubio, José R. Patiño Sánchez, Ing. Ivonne Martín M. "Desarrollo de Políticas de Seguridad Informática e Implementación deCuatro Dominios en Base a la Norma 27002 para el Áreade Hardware enla Empresa UniplexSystems S.A. en Guayaquil", Facultad de Ingeniería en Electricidad y Computación "FIEC"Escuela Superior Politécnica del Litoral "ESPOL", pp.2.

[7] ISO/IEC 27002, "Gestión de Activos de la Información".

[8] S. Chen, B. Mulgrew, and P. M. Grant, "A clustering technique for digital communications channel equalization using radial basis function networks," IEEE Trans. Neural Networks, vol. 4, pp. 570–578, July 1993.

[9] J. Ignacio Criado, MilaGascó y Carlos E. Jiménez , "Bases para una Estrategia Iberoamericana de Interope-rabilidad Documento para la consideración de la XII Conferencia Iberoamericana de Ministros de Adminis-tración Pública y Reforma del Estado Buenos Aires, Argentina, 1-2 de julio de 2010, por encargo del CLAD, pp. 4

[10] Centro de Experimentación NEC Amper.LAB, "Boletín de Observación Tecnológica en Defensa Nº 18". pag. 10-11.

[11] Jorge Ferrer, Javier Fernández-Sanguino, "Seguridad informática y software libre, Estructura de Hispalinux" Hispalinux pp.3.

[12] Jorge Ferrer, Javier Fernández-Sanguino, "Seguridad informática y software libre, Estructura de Hispalinux" Hispalinux pp.3.

[13] Jorge Ferrer, Javier Fernández-Sanguino, "Seguridad informática y software libre, Estructura de Hispalinux" Hispalinux pp.4.

[14] Jorge Ferrer, Javier Fernández-Sanguino, "Seguridad informática y software libre, Estructura de Hispalinux" Hispalinux pp.5.

[15] Jorge Ferrer, Javier Fernández-Sanguino, “Seguridad informática y software libre, Estructura de Hispalinux” Hispalinux pp.8.
[16] Roger S. Pressman, “Ingeniería del Software, un enfoque práctico”, quinta edición. R.S. Pressman&Associates, Inc. pp.29
[17] Roger S. Pressman, “Ingeniería del Software, un enfoque práctico”, quinta edición. R.S. Pressman&Associates, Inc. pp.29
[18] Roger S. Pressman, “Ingeniería del Software, un enfoque práctico”, quinta edición. R.S. Pressman&Associates, Inc. pp.507
[19] Roger S. Pressman, “Ingeniería del Software, un enfoque práctico”, quinta edición. R.S. Pressman&Associates, Inc. pp.507
[20] Serge Vaudenay, “A classical introductión to cryptography, Applications for Communications Security”, Swiss Federal Institute of Technologies (EPFL). 2006 Springer Science+Business Media, Inc. pag 135