Cuarta Conferencia de Directores de Tecnología de Información, TICAL2014
Gestión de las TICs para la Investigación y la Colaboración, Cancún, del 26 al 28 de mayo de 2014

Propuesta de Implementación de una Arquitectura Segura para activos de información de la Universidad de Boyacá

Martha Isabel Suárez Zarabanda

Universidad de Boyacá -
División de Informática Tecnología y Telecomunicaciones DINTEL
Misz38@uniboyaca.edu.co

Resumen. El proyecto relacionado a continuación involucra un trabajo institucional direccionado por la Rectoría e implementado por la División de Informática, Tecnología y Telecomunicaciones (DINTEL), como dependencia encargada de apoyar procesos académicos, administrativos y financieros de la universidad haciendo uso de los recursos de tecnología e información (IT); esta propuesta tiene como objetivo primordial Implementar una arquitectura segura para los activos de información de la Universidad de Boyacá a partir de un modelo de arquitectura de seguridad de información institucional, basado en las necesidades de seguridad de la organización y logrado a través de la implementación de unas fases metodológicas que parten del estudio institucional de la organización en cuanto al manejo de seguridad, la identificación de activos de información y sus vulnerabilidades y la propuesta de un modelo de arquitectura de seguridad de información basado en los modelos propuestos propuesto por Jan Killmeyer Tudor y por la NTC-ISO/IEC 27001:2006, su implementación y la definición de una arquitectura que asegura los activos y respalda los procesos institucionales.

Palabras Clave: Arquitectura de Seguridad de la Información, sistema de gestión de la seguridad de la información (SGSI), vulnerabilidad, gestión del riesgo.

1 Introducción

Todas las organizaciones sin importar el tipo, tamaño o función misional deben encontrarse y enfrentarse a situaciones desde o fuera de ella que generan incertidumbre a la hora de saber la continuidad del negocio y cumplimiento de sus objetivos. Esta incertidumbre vista desde la organización constituye un "riesgo".

Por ello, la información cobra al interior de la organización un valor incalculable a la hora de manejar el negocio y direccionar sus metas, y se convierte en una herramienta estratégica que permite su estabilidad, exigiendo de quienes la gestionan la responsabilidad y manejo necesario para garantizar su confidencialidad, integridad y disponibilidad.

Para dar cumplimiento a esta responsabilidad, la información debe ser gestionada en todos los niveles de la organización, por esto es importante garantizar que quienes lo hagan tengan el conocimiento necesario para hacerlo y esto sólo se cumple si al interior se tienen definidas directrices políticas y objetivos claros que orienten el manejo de la información y su seguridad.

De esta manera nace la necesidad de generar un proyecto institucional que tenga como objetivo asegurar los activos de información de la Universidad de Boyacá, apoyado en la definición de acciones de tipo gerencial, administrativo, tecnológico y técnico, con el fin de garantizar que la información se encuentre asegurada en el momento que sea utilizada para procesos misionales, productividad o funcionales en la organización.

2 Objetivos del proyecto

2.1. Objetivo general. Implementar una arquitectura segura para los activos de información de la Universidad de Boyacá a partir de un modelo de arquitectura de seguridad de información, basado en las necesidades de seguridad de la organización.

2.2 Objetivos específicos

Realizar el levantamiento de información referente al estado actual de la seguridad en la Universidad de Boyacá, con el fin de reconocer las necesidades organizacionales de seguridad.

Identificar los activos de información de la Institución junto con sus vulnerabilidades con el fin de definir su arquitectura de seguridad basada en el modelo propuesto.

Definir un modelo de arquitectura de seguridad institucional basado en las necesidades de seguridad la organización y estándares del área con el fin aplicarlo en la gestión de los activos de información de la Institución.

Desarrollar las actividades, definidas en el modelo de arquitectura de seguridad de información con el fin de implementar la arquitectura segura de los activos de información.

3 Tópicos generales

3.1 Conceptos generales de seguridad de la información.

Seguridad de la información. En la actualidad preservar, mantener, disponer y custodiar la información de una organización se ha convertido en una tarea primordial de las organizaciones y por ende de quienes la administran y gestionan la tecnología para hacerlo. Esta tarea se ha convertido en un punto determinante en el momento de cumplir los objetivos misionales de la institución y lograr su posicionamiento en el mercado actual sin importar el sector de actividad en el que se desenvuelve.

Por ello, es importante generar al interior procesos que proporcionen seguridad a la información, que según ISO 27001[1], *consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.*

¿ Características esenciales de la información segura. La información vista de manera segura deberá poseer tres características primordiales: ser íntegra, estar disponible y preservar su confidencialidad.

Según la norma ISO 27001[2], la confidencialidad contemplada como la no disponibilidad de la información a usuarios o procesos no autorizados para utilizarla; la integridad, como *la exactitud y coherencia de los datos almacenados, evidenciada por la ausencia de datos alterados entre dos actualizaciones de un mismo registro de datos.* [3] y por último la disponibilidad, como la garantía de contar con la información cuando un usuario o proceso lo requiera.

Qué aspectos se deben evaluar para dar seguridad a un activo de información? Es importante partir de las necesidades que surgen en una organización con el fin de definir una arquitectura segura que involucra no solo inversión tecnológica sino además definición de políticas y artefactos procedimentales para apoyarla y gestionarla, por ello se parte de la revisión de los siguientes aspectos:

1. Los ataques a la seguridad a los que se exponen los activos de información. La organización apoyada en quienes administran la tecnología deben identificar claramente los ataques informáticos a los cuales se encuentran expuestos los activos de información, para ello se vale del análisis de la información, infraestructura y de la gestión aplicada a ella.

2. De qué manera se contrarrestan los ataques de seguridad. Es importante que una vez se hayan identificado y analizado aquellos posibles ataques, la organización defina los mecanismos necesarios para mitigarlos, que involucra actividades técnicas, procedimentales y de gestión.

3. Cuáles servicios de seguridad/tecnológicos se pueden generar. Todos los cambios a nivel técnico implican nuevos servicios tecnológicos que pueden cubrir sólo el área de seguridad o que complementan algunos servicios que la organización ya tenía plenamente establecidos.

¿Qué es una arquitectura de seguridad a la información? Para poder tener un acercamiento a la definición de este concepto primero es necesario hablar del riesgo, *pues no es más que la posibilidad de que obtengamos un resultado distinto al que pretendíamos conseguir con nuestra acción.* [4], en una organización visto como aquella posibilidad de generar inconvenientes o resultados no deseados, luego de realizar actividades, aplicar procedimientos o ejercer una labor que conlleve a la organización a pérdidas económicas, de activos o incluso de recurso humano, asimismo ha cobrado gran importancia el concepto de activo de información, que según la ISO 17799:2005 hace referencia *algo a lo que una organización directamente le asigna un valor y por lo tanto la organización debe proteger* [5], estos activos cobran valor en el momento en que son imprescindibles cuando se llevan a cabo procesos misionales o servicios y que tienen que ver directamente con

el cliente de la organización, o cuando son necesarios para procesos que sirven de apoyo en el cumplimiento de la misión institucional.

Luego de retomar dichos conceptos, se observa claramente en qué punto y cuál es la función de una arquitectura segura en una organización, vista como una fusión de tres escenarios necesarios: la normativa de seguridad, la estructura organizativa de seguridad y la infraestructura tecnológica que las apoya, cuyo resultado conseguirá que los riesgos inherentes al manejo y administración de información en este caso, se mitiguen, controlen o se eliminen del escenario organizacional.

¿Qué busca una arquitectura de seguridad de información? La implementación de servicios de una arquitectura segura, estarán orientados a reducir vulnerabilidades o amenazas que pueden sufrir los activos de información de una organización; buscando proteger los sistemas, garantizando las características esenciales de la información, así como la detección de intrusiones a los mismos o ingresos mal intencionados a los diferentes elementos que hacen parte de la infraestructura tecnológica, como sistemas de información, redes de comunicaciones, servidores, ordenadores entre otros con los que cuenta la organización.

Dichas labores y servicios deben ir acompañados de procesos, procedimientos y actividades administrativas, alineados por una política institucional de seguridad que cubra la gestión de la seguridad de todos los activos de información identificados plenamente, gestionando y mitigando los riesgos inherentes a ellos, y proporcionando continuidad al negocio cumpliendo parcial o totalmente las leyes o normas que rigen los controles de seguridad a nivel organizacional.

¿Qué es un sistema de gestión de la seguridad de la información? Si bien la arquitectura de seguridad implica en su mayoría conceptos técnicos, no lograría su fin si no se tienen todos aquellos tópicos administrativos mencionados anteriormente y allí radica la diferencia y el punto clave para que funcione, no sirve poseer todas las condiciones técnicas necesarias sin la gestión y mantenimiento en el tiempo y esto sólo se consigue con una dinámica de seguridad continua que para este caso puede ser a través de la definición de un sistema de gestión de la seguridad de la información (SGSI), propuesto por la serie 27000 de la ISO(Organización Internacional para la Estandarización) con su principal norma ISO27001, la cual *define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande* [6], y ofrece *un estándar internacional que proporciona un modelo para establecer, implementar, utilizar, monitorizar, revisar, mantener y mejorar un SGSI* [7], el hecho de implementar actividades de monitoreo y revisión garantiza que el sistema se mantenga y además se mejore con lo observado y analizado, incidiendo de esta forma en la disponibilidad de los servicios tecnológicos y el cumplimiento de objetivos misionales.

¿Qué se puede mitigar a través de una arquitectura de seguridad y su sistema de gestión? Los activos de información de una institución pueden verse afectados por dos causas, la primera son las amenazas a las que se encuentran expuestos la cual se puede definir *como todo elemento o acción capaz de atentar contra la seguridad de la*

información[8], en una organización se percibe que los activos de información se encuentran expuestos desde el momento de su implementación, el hecho de ser elementos informáticos logra ser un blanco de amenazas tecnológicas que pueden provenir desde o fuera de la institución, existen otra amenazas que involucran los espacios físicos donde se encuentran alojados o ubicados dichos activos, y por último aquellos incidentes que se pueden presentar en la operación del activo, y la manipulación por parte del recurso humano que lo gestiona o los usuarios que lo usan. Asimismo cobran la misma importancia las vulnerabilidades que se asocian con cada activo de información, que son aquellas *debilidades que son errores potenciales que presenta un problema potencial, es decir una condición de debilidad que le permite a una amenaza producir un daño a la organización* [9], y que se relacionan con la falta seguridad del recurso humano por su inexperiencia, poco conocimiento o manejo de la seguridad, además se ligan con la carencia o implementaciones deficientes de subsistemas técnicos asociados a los activos de información como lo son la seguridad física, el control de accesibilidad al activo, el desarrollo de activos de información bajo estándares seguros, y la gestión de información en ambientes de comunicaciones, aseguramiento, respaldo y contingencia entre otros.

3.2 Arquitecturas y modelos de la seguridad de la información.

En el área tecnológica, han surgido diferentes modelos y propuestas que hacen referencia a lo que se debe realizar y tener en cuenta a la hora de proporcionar seguridad a la información de una organización, a continuación se presentan algunos de estos modelos que fueron analizados al interior de la Universidad de Boyacá, como etapas previas del proyecto de arquitectura segura y que son base del desarrollo del proyecto al interior de la Institución.

Se inició analizando el modelo propuesto por Jan Killmeyer Tudor[9] y plasmado en la siguiente figura:

Fig 1. Basado en el Modelo de Arquitectura de Seguridad de Información, planteada por el autor Jan Killmeyer Tudor através de su libro: Information Security Architecture: An Integrated Approach to Security in the Organization

Como se puede observar en el gráfico anterior, la arquitectura propuesta la componen elementos que están relacionados con la organización, el área tecnológica, los clientes o usuarios y la calidad del proceso. Por ello, la articulación de la institución y la implementación de la arquitectura, garantiza que ésta sea un apoyo de las funciones naturales en pro de objetivos y la misión organizacional, asimismo, juega un papel importante la alta gerencia como fuente del negocio, de sus necesidades y del funcionamiento como origen para la implementación deseada; a través de la *política, estándares y procedimientos* se concretan todas aquellas necesidades de seguridad de la información, que son requeridas por la organización y entregados por la alta gerencia, proporcionando directrices/procedimientos que encaminen las actividades técnicas y administrativas que involucra la propuesta de arquitectura segura, dotando a la organización de lineamientos que se rigen con buenas prácticas tanto para quienes administran los servicios de seguridad como para quienes los usan y que aseguren los objetivos misionales; lo anterior se complementa con la *línea base de seguridad y la evaluación del riesgo*, que son las especificaciones iniciales de seguridad que da la organización y bajo las cuales la arquitectura debe trabajar como objetivo, definiendo los activos de información, sus vulnerabilidades y riesgos relacionados, que alinean y delimitan el desarrollo del proyecto, que podrá posteriormente ser manejado en diferentes fases en el tiempo.

Una vez definidos la política, estándares, procedimientos bajo lineamientos institucionales y técnicos, se procede a la divulgación y expansión de conocimiento de dicha arquitectura a todos los actores de la organización por medio de la *concientización y capacitación de usuarios*, para lograr obtener los resultados esperados y mitigar los riesgos que presentan los activos de información de la institución; por último la eficacia de una arquitectura segura se mide en el tiempo y es por ello que el proyecto debe implementar procesos/procedimientos que permitan la medición de sus resultados y garantice su efectividad en la organización que constantemente varía en el tiempo.

Teniendo en cuenta que existen diferentes modelos propuestos de arquitectura de seguridad de la información, se procedió a analizar el propuesto por la NTC-ISO/IEC 27001:2006, debido a que al interior de la institución se definió el Sistema de Gestión de Calidad basado en la norma ISO 9001:2008, para aprovechar el conocimiento respecto a la norma y la forma de implementarlo; ISO 27001, está formada por once dominios relacionados con[10]: política de seguridad, organización de la información de seguridad, administración de recursos, seguridad de los recursos humanos, seguridad física y del entorno, administración de las comunicaciones y operaciones, control de accesos , adquisición de sistemas de información, desarrollo y mantenimiento , administración de los incidentes de seguridad administración de la continuidad de negocio y cumplimiento (legales, de estándares, técnicas y auditorías) y que en conjunto comprenden las áreas de[4]: sistema de gestión de la seguridad, valoración de riesgos y controles, y que se orienta bajo un ciclo de vida que define actividades de *"planear(plan), hacer(do) chequear(check) y actuar(act)"*

[11], orientadas a implementar la calidad en un proceso de gestión como lo es el proyecto de arquitectura de seguridad de la información y que lo apoyaría en etapas de monitoreo y control especialmente.

3 Metodología propuesta para el proyecto

Este proyecto generó fases metodológicas que apoyan el cumplimiento del modelo propuesto, ya que la información base como estado de la seguridad en la institución, reconocimiento de activos de información, estado de servicios tecnológicos y de seguridad no se conocían y era necesario partir de un estado actual y de necesidades reales de la Universidad de Boyacá así lograr una arquitectura segura acorde con la Institución.

Fase 1: Análisis GAP de la Universidad de Boyacá. Para identificar los riesgos asociados a la Universidad de Boyacá, se inició por un estudio de GAP Análisis Vs. las buenas prácticas internacionales en gestión de seguridad de la información, fundamentadas en la norma ISO 27001, incluyendo el tema de calidad desde la recolección de información.

Fase 2: Identificación de activos de información de la Universidad de Boyacá. Reconocer los activos de información de la Universidad de Boyacá es una tarea primordial, por ello con base en información institucional y el trabajo realizado en la DINTEL, se identificaron los activos de información manejados y custodiados directamente en la dependencia, dejando para una segunda fase aquellos administrados/custodiados por otras dependencias, estos activos fueron calificados bajo tres conceptos, confidencialidad, integridad y disponibilidad.

Fase 3. Análisis de vulnerabilidades de activos de información de la Universidad de Boyacá. El análisis de vulnerabilidades sobre las plataformas seleccionadas por la Universidad de Boyacá tiene como fin, validar que la implementación de la infraestructura tecnológica que se encuentra disponible, cumpla con la seguridad adecuada, de tal manera que la identificación previa de vulnerabilidades y el reconocimiento de soluciones logre mitigar incidentes y riesgos que puedan afectar la integridad, disponibilidad y confidencialidad de la organización.

Las recomendaciones y consideraciones que deberán ser tenidas en cuenta por el proyecto, no obedecen a la implementación de algún método y/o tecnología en particular, corresponden a recomendaciones internacionales sobre las mejores prácticas en seguridad de la información y buscan garantizar el tratamiento idóneo de la información, basados en el modelo propuesto por el proyecto.

Fase 4. Modelo de implementación de arquitectura de seguridad de activos de información de la Universidad de Boyacá. Con la información que arrojan las fases previas se inicia la implementación del proyecto de arquitectura de seguridad con el fin de generar todas aquellas estrategias de tipo físico, tecnológico y administrativo para garantizar el cumplimiento de los objetivos del proyecto.

4 Avance del proyecto

En la actualidad el proyecto ha superado las tres primeras fases determinando de esta manera la información necesaria para ejecutar las fases del modelo propuesto, asimismo se ha iniciado con el desarrollo del modelo de implementación de arquitectura de seguridad de activos de información de la Universidad de Boyacá.

4.1 Fase 1: Análisis GAP de la Universidad de Boyacá. Como se mencionó anteriormente esta fase hace uso de un análisis GAP , que permitió comparar los procesos actuales de seguridad de la Universidad con respecto al estándar ISO 27001 se realizó una revisión de los 133 controles y sus respectivos sub-controles de la norma se establecieron los puntajes apropiados para cada uno de los controles recomendados versus los actuales controles, en éste análisis se identificaron áreas en las cuales se debía mejorar y como lo demuestra la figura No. 2 , dicha herramienta fue aplicada directamente a la información y recurso humano de la división de informática, tecnología y telecomunicaciones.

La razón de este enfoque inicial se da debido a que los posibles impactos relacionados con la información dependen de tres factores fundamentales existentes en todas las organizaciones, como son: Las personas, los procesos y la tecnología que deben ser analizados bajo los principios de la seguridad de la información que son la Confidencialidad, Integridad y Disponibilidad. [13]

Los resultados del análisis de GAP se plasman en la siguiente figura y conclusiones generales:

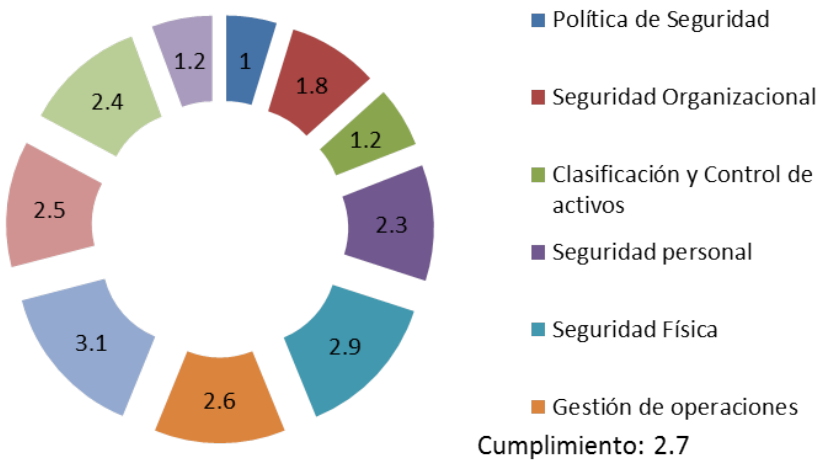

Fig. 2. Representación análisis GAP de la Universidad de Boyacá.

4.1.1 Conclusiones generales [13]**:** Se detectan varias no conformidades de acuerdo a la norma, el detalle de estas se establece en el capítulo de GAP Análisis Vs. la norma ISO 27001.

Según este GAP análisis realizado, el nivel de madurez versus las buenas prácticas no es el apropiado para una entidad como la Universidad de Boyacá donde se gestiona información privada y confidencial de su alumnado. Es claro que entidades como la Universidad de Boyacá tiene dentro de sus valores corporativos la transparencia y seriedad en la gestión de la información.

Los cuatro puntos más inquietantes son:

1. Política de Seguridad. No existen políticas formales sobre seguridad de la información. Se debe definir una política clara alineada con los objetivos de negocio de la Universidad de Boyacá, esta política debe ser apoyada con un sistema de gestión que garantice su cumplimiento.

2. Seguridad Organizacional. Se debe crear un comité gerencial de Seguridad de la Información que se encargue de promover las iniciativas de Seguridad de la Información dentro de la organización, así como obtener los recursos necesarios para dichas actividades.

3. Seguridad del Personal. Debe iniciarse un proceso de concientización y culturización sobre seguridad de la información a todos los empleados directos, indirectos y contratistas de la Universidad de Boyacá.

4. Gestión de la continuidad del negocio. Es importante tener sistemas totalmente redundantes y de alta disponibilidad en la infraestructura de servidores tanto a nivel interno en el centro de cómputo como en un centro alterno de contingencia. Sistemas redundantes que permitan establecer un RTO (Tiempo de Retorno Objetivo) apropiado para no impactar significantemente la parte financiera y de reputación o imagen de la Universidad de Boyacá.

4.2 Fase 2: Identificación de activos de información de la Universidad de Boyacá. Como se ha mencionado anteriormente para la identificación de los activos de información necesarios se analizaron aquellos activos administrados /custodiados por DINTEL, ya que allí reposan elementos que hacen parte de la infraestructura tecnológica de la Institución y apoyan o prestan servicios tecnológicos que respaldan los procesos académicos y administrativos de la universidad, dentro de dichos activos ser encuentra servidores de información, que contienen bases de datos que manejan información académica, financiera y administrativa, equipos activos que soportan todo el sistema de comunicación institucional y otros activos que soportan servicios requeridos por diferentes estamentos de la organización.

Estos activos fueron valorados bajo tres ítems: confidencialidad, integridad y disponibilidad, generando con ello un valor a cada activo y una clasificación de acuerdo a ello, hallando activos con clasificación Muy Alto (17 activos de información), Alto (1 activo) y Medio (3 activos).

Los activos que recibieron la mayor calificación están relacionados con los sistemas de información que posee la Universidad de Boyacá como servidores de aplicaciones o servidores donde se alojan bases de datos institucionales, otros que proveen servicios de seguridad como Firewall, directorio activo y por último los equipos activos de mayor impacto como el Switch de core de la sede principal, en nivel medio se encuentra los activos relacionados con entorno de desarrollo y el medio relacionados con los switchs de borde que conforman la red de comunicaciones

4.3 Fase 3. Análisis de vulnerabilidades de activos de información de la Universidad de Boyacá. El análisis fue aplicado a cada uno de los activos administrados/custodiados por DINTEL, a equipos de cómputo de usuarios finales en diferentes sistemas operativos y comunicaciones externas, esta documentación tuvo como alcance la identificación de las vulnerabilidades en cada uno de los activos así como la solución que permita mitigar sus riesgos, asimismo las evidencias correspondientes que soportan la información.

Para este análisis se utilizaron herramientas para la evaluación de sistemas operativos, exploración de la red, servicios sobre la red, pruebas al perímetro de la infraestructura, entre otras.

4.4 Fase 4. Modelo de implementación de arquitectura de seguridad de activos de información de la Universidad de Boyacá

Definición del Modelo. La generación de la arquitectura de seguridad es un proyecto institucional que está relacionado con todos los estamentos de la Universidad de Boyacá, desde la alta gerencia, las dependencias usuarias de los activos de información y la dependencia encargada de administrarlos, por ello debe abarcar además de los ítems técnicos, aquellos relacionados con su gestión bajo estándares de calidad y cumplimiento que la fusión de los modelos de arquitectura de seguridad de información mencionados en el capítulo de tópicos generales y plasmados en la figura 2 proporcionan.

Esta fusión garantiza el acercamiento del proyecto a las necesidades a partir del conocimiento de la información institucional generando de esta forma el marco teórico institucional que se plasma en la política de seguridad estándares y procedimientos requeridos para implementar y gestionar servicios de seguridad y aquellos técnicos o de gestión requeridos para prestarlos y mantenerlos por medio de acciones que verifiquen sus resultados e implementen actividades de mejoras en los casos necesarios.

Por último la implementación del proyecto de la arquitectura segura vista con la figura anterior, deberá proponer a partir de la línea base de seguridad y la evaluación de riegos de los activos de información de la institución, la política, estándares procedimientos, servicios de seguridad y tecnológicos requeridos por la Universidad de Boyacá.

Cada una de las fases que permitirán la definición de la arquitectura de seguridad de los activos de información, están acompañadas de acciones y actividades que enmarcan la mejora continua con el “planear (plan), el hacer (do) el chequear (check) y el actuar (act)” además, se observa la integración del proyecto con la organización, la intervención de los resultados en la solución a las necesidades de seguridad y la vinculación de los actores a través de la concientización, por ello se consideró que la fusión de los modelos garantiza la generación de una política institucional de seguridad que enmarca, procedimientos, estándares y acciones técnicas, administrativas y tecnológicas orientadas a garantizar la confidencialidad, integridad y disponibilidad de los activos de la información de la Universidad de Boyacá.

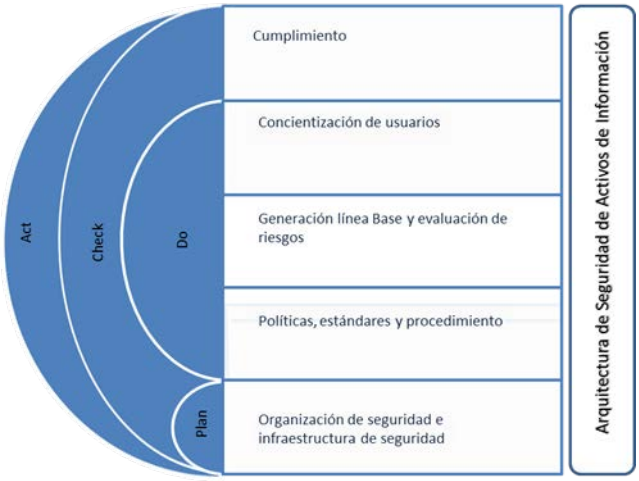

Fig. 2. Modelo de Implementación de Arquitectura de Seguridad de Activos de Información de la Universidad de Boyacá, propuesta por la autora basada en los modelos de Jan Killmeyer Tudor y la NTC-ISO/IEC 27001:2006.

5 Consideraciones técnicas generadas a partir del proyecto

Uno de las grandes áreas del proyecto ha sido lo relacionado con la actualización técnica de la infraestructura tecnológica de la Universidad de Boyacá, que ha requerido de varios recursos: humanos, económicos y técnicos para lograr los objetivos. Cuando se percibe la necesidad de asegurar los activos de información de la Universidad de Boyacá, DINTEL inicia un trabajo de revisión de la infraestructura tecnológica para garantizar los cambios en la misma. Esta revisión permitió identificar los siguientes hallazgos:

5.1 Condiciones generales iniciales de infraestructura. La evaluación inicial arrojó los siguientes datos: diecisiete servidores de diferentes marcas, configuraciones y la mayoría obsoletos y sin soporte.

Una UPS para el soporte de varios de estos

Un Centro de cableado sin condiciones mínimas técnicas para este tipo de espacios

Tendido de cableado Cat 6ª, en óptimas condiciones

La Red LAN, Switches de Core y Switches de borde, de muy buenas especificaciones.

5.2 Labores realizadas. *Subsistema Obra Civil*: Este subsistema involucró actividades de adecuación física del data center en cuanto a cerramiento, manejo de luz, piso especial para data center, y adecuaciones eléctricas para ello, además el data

center fue equipado con UPS, aire de precisión, actualización de PBX y sellamiento de ducterías de data center.

Subsistema Servidores: Se migran los servidores de la Institución a un servidor Blade IBM, con servidores IBM tipo blade, apoyados con almacenamiento tipo SAN, y Sistema de Back up Tape

Subsistema de virtualización y consolidación de servidores: Se instaló una plataforma de virtualización que permitió la migración de todos los servidores y sus servicios bajo dicho esquema, además se hizo la migración de la base de datos del sistema integrado de información a la plataforma de Oracle RAC 11g.

Subsistema de seguridad: Se debió rediseñar la configuración de la red de comunicaciones de la institución implementando protocolos de seguridad como el 802.1x, servicios de Host Integrity check, firewall de aplicaciones, servicio en las redes cableada e inalámbrica de portal cautivo, protector de base de datos no intrusivo, integración de aplicaciones mediante “single sign on” con el aplicativo ADAS entre otros.

Como se puede observar la seguridad de los activos de información en una organización como la Universidad de Boyacá requirió de cambios drásticos en la configuración y por ende gestión de la infraestructura tecnológica, llevando al grupo de DINTEL a la creación un modelo de arquitectura de seguridad y un sistema de gestión que lograsen complementar dichos cambios y gestionarlos en el tiempo, además es importante resaltar el proceso de capacitación y auto capacitación requerida para lograrlo.

5 Impacto del proyecto

Se debe resaltar inicialmente que este proyecto se encuentra en ejecución aún debido a la magnitud de su definición, implementación y adecuaciones técnicas relacionadas con hardware y software

La generación de un modelo de arquitectura de seguridad de la información y su apoyo a través de un sistema de gestión de la seguridad han incido positivamente en la organización ya que debido al proyecto se ha iniciado un trabajo de "cultura de la seguridad" que inicialmente impactó a los integrantes de DINTEL permitiendo la generación de nuevos servicio tecnológicos, implementación de nuevos elementos tecnológicos que se ven reflejados en el aseguramiento de la infraestructura, y sobre todo la cultura de la documentación, pieza clave a la hora de gestionar y mantener un servicio, asimismo en diferentes niveles se han creado políticas procedimientos y estándares que garantizan la continuidad de los servicio y la mejora continua de los mismo.

Estas ventajas se han proyectado a la organización debido a que los activos de información se encuentran en proceso de actualización y están sometidos a una gestión basada en políticas, procedimientos y mejora continua, relacionando directamente a los actores y usuarios quienes han empezado a reconocer la importancia del tema de aseguramiento de la información en la organización.

6. Conclusiones

Un proyecto que tiene como finalidad la generación de una arquitectura segura para los activos de información de una organización como la Universidad de Boyacá, debe ser apoyado por la alta gerencia en este caso la rectoría y reconocido institucionalmente, para lograr su despliegue en todos los estamentos de la institución.

El diseño y desarrollo del proyecto de Arquitectura segura y su SGSI, deben basarse en las necesidades de seguridad organizacionales, para garantizar su eficacia en las reglas del negocio y su apoyo en la continuidad del mismo, influenciados por la misión, objetivos misionales, estructura de la organización y usuarios de los activos de información.

El modelo propuesto de arquitectura de seguridad de la información fusionó dos modelos que garantizan las buenas prácticas de la seguridad de la información y la inclusión de la calidad y el mejoramiento continuo en las fases propuestas, respondiendo a las necesidades de seguridad identificadas en la Universidad de Boyacá.

El modelo propuesto incluye fases de cumplimiento que reflejan el seguimiento y la mejora continua en los procedimientos actividades o acciones definidas, lo que exige por parte de DINTEL como unidad de despliegue, un compromiso permanente en el análisis de amenazas y vulnerabilidades de los activos de información para garantizar el objetivo de este proyecto.

Agradecimientos

Este trabajo ha sido financiado por la Universidad de Boyacá en su totalidad

La autora desea expresar su agradecimiento a la Dra. Rosita Cuervo Payeras, rectora de la Universidad de Boyacá

Referencias

1. Portal de ISO 27.000 en español, http://www.iso27000.es/download/doc_sgsi_all.pdf

2. Portal Área de Ciencias de la Computación e Inteligencia Artificial de la Universidad de Vigo, http://ccia.ei.uvigo.es/docencia/SSI/normas-leyes.pdf

3. Gelbstein, Ed, Data Integrity—Information Security's Poor Relation. J. Isaca. Vol 6, 20 a 25 (2011)

4. Pontificia Universidad Católica del Perú, http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/4957/ESPINOZA_HANS_ANALISIS_SISTEMA_GESTION_SEGURIDAD_INFORMACION_ISO_IEC%2027001_2005_COMERCIALIZACION_PRODUCTOS_CONSUMO_MASIVO.pdf?sequence=1

5. Universidad Complutense de Madrid http://pendientedemigracion.ucm.es/info/jmas/mon/20.pdf

6. ISO 270001 and ISO 22301 Online Consultation Center, http://www.iso27001standard.com/es/que-es-la-norma-iso-27001

7. Estrada, Y., Wilson, A., Anety, M.: Fundamentos para implementar y certificar un Sistema de Gestión de la Seguridad Informática bajo la Norma ISO/IEC 27001 ACIMED [online] . Vol 5, No. 10 (2012)

8. Universidad Nacional de Lujan http://www.scielo.org.ve/scielo.php?pid=S1690-75152009000100004&script=sci_arttextur documents with ease.

9. De Freitas, Vidalina.: Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar [online] . Vol 6, No. 1 pp 43-55 (2009)

10. Tudor, Jan Killmeyer: Information Security Architecture: An Integrated Approach to Security in the Organization . En: Estados Unidos, Auerbach, 2ª Edición, 393,(2006)

11. Universidad de las ciencias informáticas http://publicaciones.uci.cu/index.php/SC

12. Global Knowledge, Project Management Professional (PMP). PMI. Vol 1, 129 a 130 (2013)

13. Universidad de Boyacá, Itelca: Informe Final GAP_ISO27001-UBOYACA v 1 0, pp 1 (2012)