Universidad de Boyacá

Tunja -
Colombia

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

Martha Isabel Suárez Zarabanda

Cancún – México

2014

SEGURIDAD DE LA INFORMACIÓN

FUENTE:

AGENDA

- Introducción
- Objetivos de Proyecto
- Metodología propuesta para el proyecto
- Avance del Proyecto
- Consideraciones Técnicas generadas a partir del Proyecto
- Conclusiones

INTRODUCCIÓN

- Las organizaciones deben enfrentarse a situaciones desde el interior o fuera de ellas, que generan incertidumbre acerca de la continuidad del negocio y cumplimiento de sus objetivos, esta incertidumbre constituye un “riesgo”.

- La información un valor incalculable a la hora de manejar el negocio y direccionar sus metas, se convierte en una herramienta estratégica que permite la estabilidad de una organización.

- Por ello la importancia de la gestión de la *información* en todos los niveles de la organización con acciones de tipo gerencial, administrativo, tecnológico y técnico que la aseguren y garanticen la *integridad, disponibilidad y confidencialidad*

OBJETIVOS DEL PROYECTO

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

Levantamiento de información institucional	→	Necesidades de Seguridad
Identificación Activos de información y sus Vulnerabilidades	→	Arquitectura de seguridad basada en el modelo propuesto
Definir un modelo de arquitectura de seguridad institucional	→	Gestión de los activos de información de la Institución
Desarrollar las actividades definidas en el modelo propuesto	→	Implementar la arquitectura segura

METODOLOGÍA PROPUESTA PARA EL PROYECTO

Fase 1
- Análisis GAP de la Universidad de Boyacá

Fase 2
- Identificación de activos de información de la Universidad de Boyacá

Fase 3
- Análisis de vulnerabilidades de activos de información de la Universidad de Boyacá

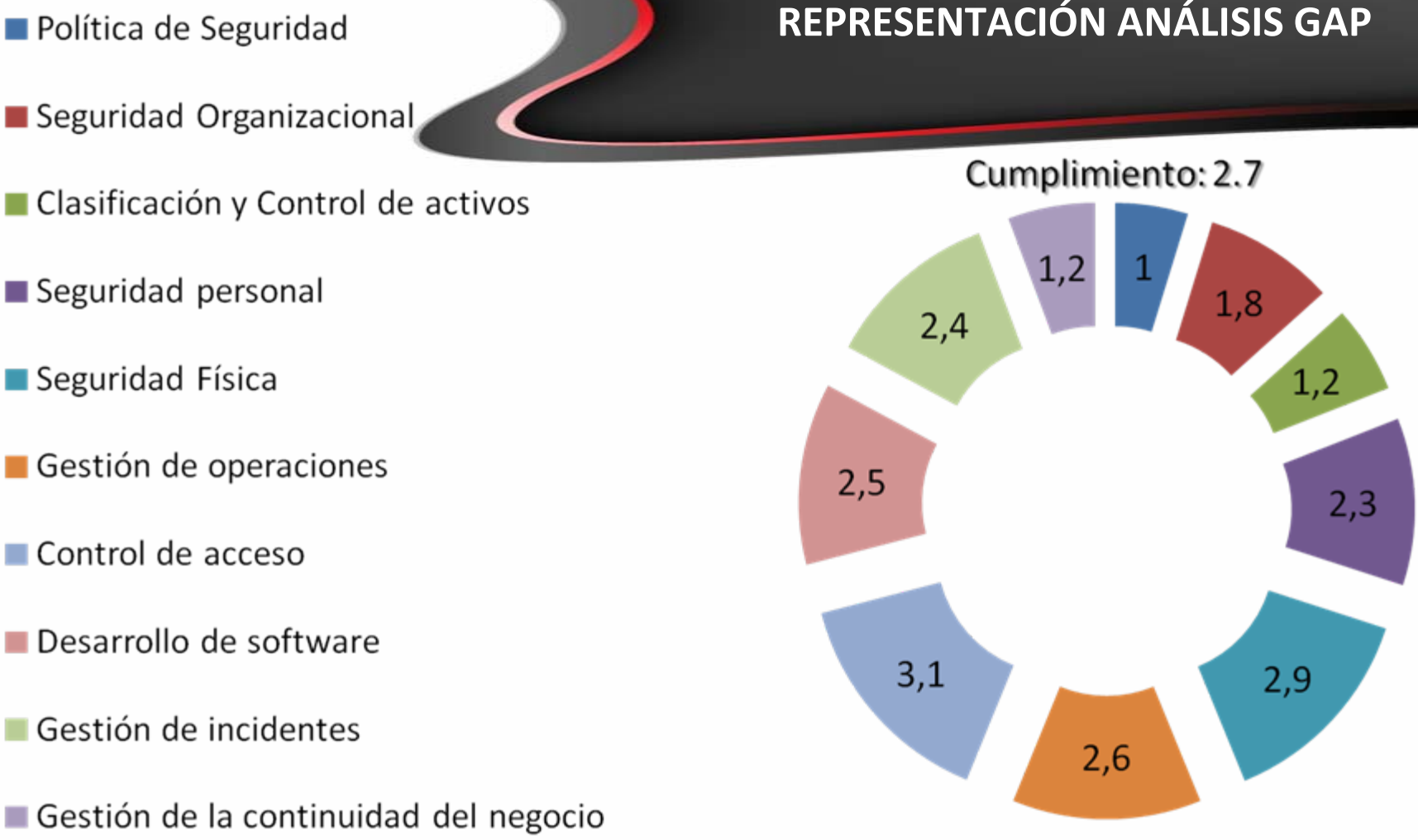
Fase 4
- Modelo de implementación de arquitectura de seguridad de activos de información de la Universidad de Boyacá

AVANCE DEL PROYECTO

Fase 1: Análisis GAP de la Universidad de Boyacá

- uso de un análisis GAP comparar procesos actuales vr estándar ISO 27000
- Trabajo realizado a DINTEL y sus recursos: humanos , procedimentales y tecnológicos
- Conclusiones GAP
- Política de Seguridad – Seguridad Organizacional - Seguridad del Personal - Gestión de la continuidad del negocio

REPRESENTACIÓN ANÁLISIS GAP



AVANCE DEL PROYECTO

Fase 2: Identificación de activos de información

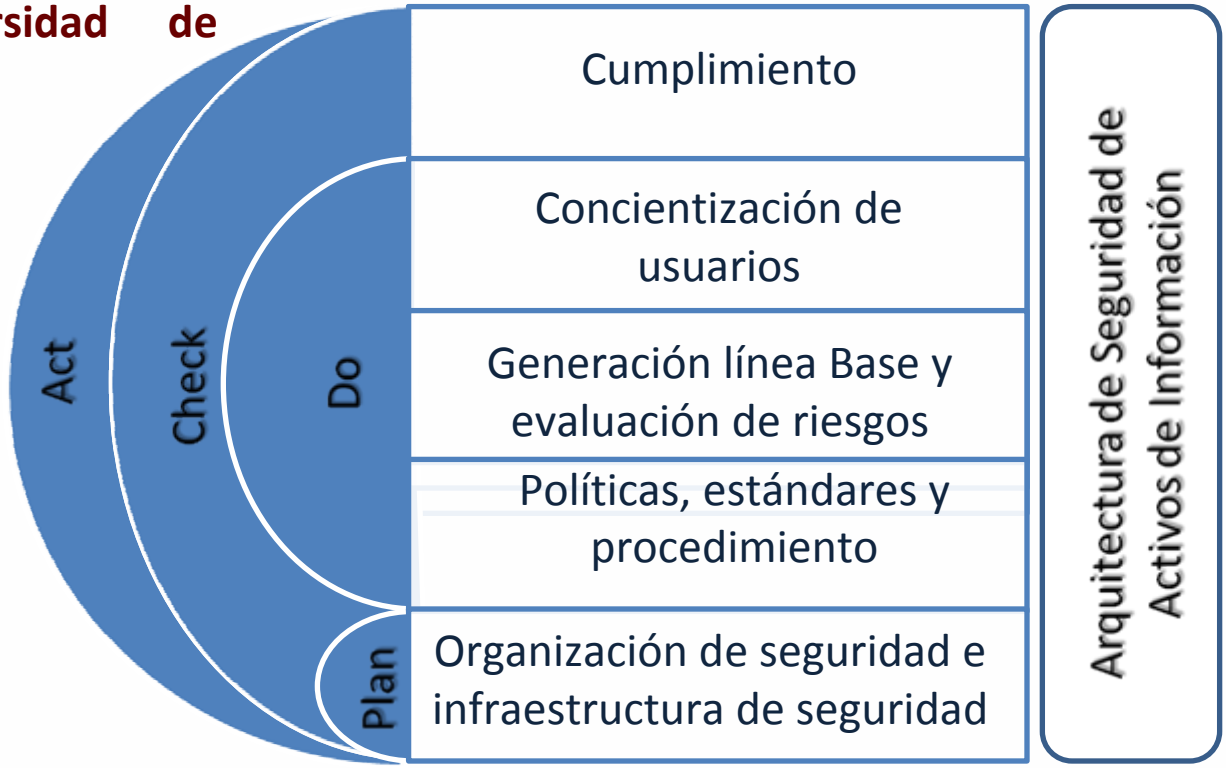
- Identificación de Activos de información: Sistemas de Información, Servidores, Activos de Seguridad – Equipos activos
- Valoración de cada activo de información: confidencialidad, integridad y disponibilidad
- Clasificación de los activos de Información

AVANCE DEL PROYECTO

Fase 3. Análisis de vulnerabilidades de activos de información

- Activos administrados/custodiados por DINTEL - equipos de cómputo de usuarios finales
- Identificación de las vulnerabilidades
- Evidencias y solución que permita mitigar sus riesgos

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



Fuente: 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.

CONSIDERACIONES TÉCNICAS GENERADAS A PARTIR DEL PROYECTO

1	*Subsistema Obra Civil*	Adecuación física del data center
2	*Subsistema Servidores*	Migración de granja servidores a sistema Blade - Almacenamiento en red(SAN) – Sistema de Back up en red
3	*Subsistema de virtualización y consolidación de servidores*	Virtualización de servicios tecnológicos, bases de datos con alta disponibilidad y balanceo de cargas

CONSIDERACIONES TÉCNICAS GENERADAS A PARTIR DEL PROYECTO

- Rediseño de la configuración de la red de datos
- Servicios de Autenticación, Autorización y Auditoría(AAA) utilizando : protocolo 802.1x - servicios de Host Integrity check – portal cautivo para red cableado e inalámbrica.
- Implementación de Firewall de aplicaciones
- Implementación Firewall de base de datos
- Implementación de punto único de autenticación a través de AD de sistemas de información(C/S, web, plataforma virtual, correo electrónico) y equipos.

CONCLUSIONES

- La generación de una arquitectura segura debe ser apoyado por la alta gerencia en este caso la rectoría para ser reconocido institucionalmente.

- El diseño y desarrollo del proyecto de Arquitectura segura y su SGSI, deben basarse en las necesidades de seguridad organizacionales.

- 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.

- El modelo propuesto incluye fases de cumplimiento que reflejan: el seguimiento, mejora continua y el compromiso permanente de quienes administran los activos de información de una organización.

¡ Muchas gracias por su atención!