

GESTIÓN DE RIESGOS DE TI.

1. INTRODUCCIÓN

Dentro de los modelos de gestión de TI soportados bajo el enfoque de procesos, gestión de riesgos y PHVA, se encuentran las normas ISO 27001, ISO 20000, ITIL y BS 25999 de seguridad de la información, gestión de servicios de TI y continuidad del negocio (BCP, DRP), respectivamente, cuya implementación debe asegurar un trabajo eficiente y orientado con las directrices estratégicas de las diferentes instituciones. La consideración simultánea de estos modelos de gestión, requiere de un proceso sincronizado de implementación que evite la duplicidad de operaciones y las estructuras burocráticas a nivel documental, de tal manera que se configure un verdadero sistema integrado de gestión alrededor de los servicios de TI. SISTESEG consiente de esta realidad ha trabajado en diseñar de forma adecuada procesos de implementación con un enfoque integral que le permita a las diferentes instituciones diseñar e implementar un sistema de gestión flexible que realmente apoye el cumplimiento de las expectativas de sus partes interesadas (Estudiantes, accionistas, empleados, profesores, proveedores, etc.), en tiempos reducidos y sin generar traumatismos en la operación diaria de la institución.

Por otro lado, la seguridad de la información y la continuidad del negocio son dos componentes críticos de la estrategia futura de muchas instituciones a nivel nacional e internacional. El desarrollo a futuro del documento de lineamientos le permitirá a las diferentes instituciones, por un lado, comprender la importancia de definir políticas, normas, procedimientos y estándares, de acuerdo a los requerimientos de su misión, basados en recomendaciones, mejores prácticas (frameworks) desarrollados con cooperación internacional, y por otro lado, se busca también, a través del desarrollo de estos lineamientos, identificar herramientas o productos

tecnológicos que apoyen los controles que permiten mitigar el riesgo y mejorar de esta manera la seguridad de la información y la continuidad de las operaciones.

Lo anteriormente expresado nos ha llevado a proponer lineamientos que consideren los aspectos fundamentales de ISO 27001, ISO 27002, ISO 27005, ISO 20000, COBIT 4.1, COSO, ITIL V3 y BS 25999, entre otros, con el fin de plantear una ruta estratégica que le ofrezca a las organizaciones la capacidad para estar mejor preparada ante un entorno cambiante y de alto riesgo. Este documento se propone pues desarrollar los lineamientos para la implementación efectiva y eficiente de estas recomendaciones internacionales y controles, promoviendo de esta forma un verdadero gobierno de TI y, por ende, de esta manera, lograr una mejor gestión del riesgo al que pueden estar expuestas hoy en día las empresas.

2. ALCANCE

Los lineamientos para los servicios de TI cubre también aspectos como: disponibilidad, desempeño, confidencialidad, integridad y controles de acceso físico, administrativos y lógicos, de tal forma que proponemos un enfoque integral de acercamiento a la gestión del riesgo y al gobierno de TI. De tal manera que se pueda combinar efectivamente la seguridad de la información en los diferentes sistemas hoy disponibles en las diferentes divisiones. Todo lo anterior conforma una estrategia integrada para la seguridad de la información y la continuidad del negocio, basado, claro está, en una estrategia efectiva de gestión de riesgos.

3. OBJETIVOS PRINCIPAL

Estos lineamientos se enfocan en ofrecer las directrices para una gestión integral de la seguridad de la información, la prestación de servicios con calidad y a la

continuidad de las operaciones¹. Se busca de esta manera generar un camino claro y expedito para luego poder emprender el desarrollo de un modelo de gestión seguridad de la información, o SGSI, un modelo de gestión de los servicios con calidad y, por último, un plan de recuperación ante desastres.

4. ASPECTOS A CONSIDERAR EN LA GESTIÓN DEL RIESGO

Criterios en seguridad de la información

- Confidencialidad
- Integridad
- Disponibilidad y Desempeño

Elementos a considerar (las cuatro P's) para un sistema de gestión de la seguridad de la información efectivo:

- Procesos
 - Gestión de riesgos
 - Manejo de incidentes
- Personas
 - Entrenamiento
 - Educación
 - Certificaciones
- Productos y tecnologías
 - Firewalls
 - Redes
- Proveedores

¹ PAS 99 es la primera especificación de requisitos del mundo para sistemas de gestión integrada que se basa en los seis requisitos comunes de la guía ISO 72 (una norma para redactar normas para sistemas de gestión). Desarrollada como respuesta a la demanda del mercado de alinear los procesos y procedimientos en una estructura holística que permitiera operar con mayor eficacia. La gestión integrada es adecuada para cualquier organización, independientemente del tamaño o sector, que quiera integrar dos o más sistemas de gestión en un solo sistema cohesionado con un conjunto holístico de documentación, políticas, procedimientos y procesos según el BSI.

✚ Estándares internacionales a considerar para realizar el documento de lineamientos

- ISO 27001
- ISO 17799
- BS 25999
- ISO 20000
- COBIT 4.1
- ITIL V3
- COSO
- ISO 27005
- M_o_R
- MOF
- AU NZ/4360
- NFPA 75
- NFPA 1600
- NIST SP 800-34

✚ Continuidad del Negocio (BCP), planes de contingencia y planes de recuperación ante desastres (DRP)

- Metodologías sugeridas
 - NIST
 - DRII
 - BCI
 - NFPA 1600
 - BS 25999
- Relación BCP y DRP
- Lineamientos para realizar un efectivo BIA²

² Business impact analysis

- DRP y categorización de amenazas
- Planes de contingencia y el NIST SP 800-34
- Estrategias de recuperación
 - Hot sites
 - Cold sites
 - Warm sites
 - Mirror
- El modelo BCM propuesto por BS 25999

 Futuro de las auditorías ISO 27001 e ISO 20000

- Requerimientos
- Certificaciones
- Beneficios para la Universidad