Arquitectura TI COLOMBIA
MARCO DE REFERENCIA

vive digital Colombia

G.ES.05 Diseño e implementación de una estrategia de seguridad de la información

Guía Técnica

Versión 1.0

29 de abril de 2015

Estrategia TI

MINTIC

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0	29 de abril de 2015	Emisión

DERECHOS DE AUTOR

AUTORA

María Isabel Mejía Jaramillo
Viceministra de Tecnologías y Sistemas de la Información
Ministerio de Tecnologías de la Información y las Comunicaciones

COLABORADORES

Jorge Fernando Lobo Bejarano
Director de la Dirección de Estándares y Arquitectura de TI
Ministerio de Tecnologías de la Información y las Comunicaciones

Asesores del Ministerio de Tecnologías de la Información y las Comunicaciones
Claudia Milena Rodríguez Álvarez
Lina Marcela Morales

Asesores de la Corporación Colombia Digital
Javier Orlando Torres Páez
Deicy Alexandra Parra Chaux
Diego Antonio Campos Cáceres
Jorge Alberto Villalobos Salcedo
Diana Piedad Gómez Castaño
Javier Alexander Mayorga Melo
Jaime Leonardo Bernal Pulido
Hermes Camilo Cubaque Barrera
Leydi Viviana Cristancho Cruz

Medios Digitales
María Astrid Toscano Villán
Ricardo Rojas Ortíz
Jhon Henry Munevar Jiménez

UT Everis Tecnocom
Alberto Pizarro Carrasco
Gerardo Antonio Moreno
Martha Lucía Parra
Martha Patricia Naranjo Becerra
David Fernando de la Peña Santana
Lucio Augusto Molina Focazzio
Silvia María Fernández Coello
Karin Xiomara Marroquín
Maribel Ariza Rojas
Ramiro Andrés Delvasto
Diego Ordóñez
Édgar Esquiaqui
Ricardo Abad Chacón Ibarra
Juliana Botero Iragorri
Juan Pablo Sequera España

TABLA DE CONTENIDO

PÁG.

LISTA DE ILUSTRACIONES

PÁG.

1. INTRODUCCIÓN

A continuación se presentan los objetivos, el alcance de la guía y se identifican los lineamientos del Marco de Referencia que apoya la misma. En el presente documento se describe la Guía para el Diseño e Implementación de la Estrategia de Seguridad de la Información para las Instituciones del Estado Colombiano.

2. OBJETIVOS DE LA GUÍA

Los siguientes son los principales objetivos:

- Estandarizar el flujo de pasos que deben seguir las instituciones, en el momento de definir y estructurar su Estrategia de Seguridad de la Información.
- Contribuir a la disminución de incidentes y problemas relacionados con la seguridad de la información.
- Facilitar la implementación de los lineamientos del Marco de Referencia, relacionados con la seguridad de la información.

3. ALCANCE DE LA GUÍA

El alcance de esta guía está definido por:

Los pasos que definen las acciones que una institución debe seguir para formular e implementar su estrategia de seguridad de la información. La guía no incluye la identificación de herramientas de seguridad de la información ni las actividades definidas para administrar estas herramientas o las operaciones a realizar dentro del ámbito de la seguridad informática.

4. LINEAMIENTOS ASOCIADOS

Esta guía es un instrumento de apoyo a las instituciones del Estado para facilitar la aplicación del marco de referencia. Esta guía contribuye a la implementación de los siguientes lineamientos del dominio Estrategia de TI, del Marco de Referencia de AE para la Gestión de TI:

- Políticas y estándares para la gestión y gobernabilidad de TI (LI.ES.06)

5. DESCRIPCIÓN

En esta sección se presentan las actividades que las instituciones deben ejecutar, para diseñar e implementar su Estrategia de Seguridad de la Información.

6. INTRODUCCIÓN AL DISEÑO E IMPLEMENTACIÓN DE LA ESTRATEGIA DE SEGURIDAD DE LA INFORMACIÓN

El objetivo de una Estrategia de Seguridad de la Información es trazar un camino que le permita a una institución llegar al estado de madurez o capacidad deseado en materia de seguridad de la información. Dicha Estrategia debe ser establecida por la organización y definida por los atributos de negocio y de seguridad de la información. Como se verá en el ciclo a seguir para diseñar e implementar la Estrategia de Seguridad de la Información, la alta dirección y el dueño del proceso deben, de común acuerdo, determinar a qué nivel de madurez o capacidad desean llevar el proceso. La Estrategia establece la base para un plan de acción que incluya uno o más programas de seguridad que, en la medida que se vayan ejecutando, logren los objetivos de seguridad de la información y permitan llevar el proceso de seguridad de la información, del nivel en que se encuentra, al nivel de madurez o capacidad esperado.

Cada plan de acción debe formularse según los recursos disponibles y las limitaciones existentes, incluyendo la consideración de requerimientos legales y regulatorios. Tanto la Estrategia, como los planes de acción, deben contener mecanismos de monitoreo y métricas definidas para determinar el nivel de éxito.

Para el diseño de la Estrategia de Seguridad de la Información, es importante entender qué significa la palabra estrategia.

Kenneth Andrews describe el concepto de estrategia corporativa la cual también es aplicable para este contexto: "la estrategia corporativa es el patrón de decisiones en una compañía, que determina y revela sus objetivos, propósitos o metas; que genera las principales políticas y planes para alcanzar dichas metas y define el rango de negocio que debe perseguir la compañía, el tipo de organización económica y humana que es o pretende ser y la naturaleza de la contribución tanto económica, como no económica, que pretende hacer a sus accionistas, empleados, clientes y comunidades". [1]

Una Estrategia de Seguridad de la Información es una decisión u opción que se elige luego de un estudio o análisis con el fin de alcanzar un objetivo. La estrategia debe contener como mínimo lo siguiente:

- Un objetivo: lo que se busca alcanzar a través de la ejecución de la estrategia.
- Acciones: actividades a ejecutar para cumplir con lo definido en la estrategia.
- Resultados: lo que se espera obtener de esas acciones que permiten cumplir con el objetivo propuesto.
- Tiempos: periodo en el cual se debe ejecutar la estrategia.
- Métricas: mecanismos para monitoreo y seguimiento a la implementación e impacto en las diferentes instituciones.

Es importante anotar que:

- Estrategia de TI puede incluir la Estrategia de Seguridad de la Información, esto se da cuando los responsables de liderar la seguridad de la información hacen parte del área de TI, como ocurre con las instituciones del Estado colombiano.

- La información es inherente a la misión de las instituciones y su correcta gestión debe apoyarse en tres pilares fundamentales los cuales deben ser considerados en la definición de la Estrategia de Seguridad de Información:

- Confidencialidad: la información debe ser sólo accesible a sus destinatarios predeterminados.

- Integridad: la información debe ser correcta y completa.

- Disponibilidad: la información debe estar disponible en el momento y lugar que se requiera.

El proceso de seguridad de la información debe velar porque la información sea correcta y completa, esté siempre a disposición del cumplimiento de las metas de la institución y sea utilizada sólo por aquellos que tienen autorización para hacerlo.

Para implementar la Estrategia de Seguridad de la Información en una institución es necesario que dicha Estrategia esté alineada con los objetivos estratégicos de la organización.

Para efectos de esta guía se utiliza la definición de "activo de información" de la norma ISO/IEC 27002:2013, dado que este concepto, para el contexto de seguridad de la información es más amplio que el definido en el decreto reglamentario de la ley 1712 de 2013 que hace referencia a la Ley de Transparencia y Acceso a la Información Pública. En concordancia, un activo de información se define cómo cualquier información, sistema de información o infraestructura tecnológica relacionada con el tratamiento de la misma que tenga valor para la organización. Entre los principales activos de información se encuentran, además de la información, las bases de datos, el software, el hardware, los contratos, los equipo de comunicaciones, los servicios informáticos y de comunicaciones, las utilidades generales como por ejemplo calefacción, iluminación, energía y aire acondicionado y las personas, que son quienes generan, transmiten y destruyen información.

7. ¿QUÉ ACCIONES DEBE SEGUIR LA INSTITUCIÓN?

Con el fin de planear la estrategia de entendimiento y adopción del Marco de Referencia de AE, la institución puede considerar realizar los siguientes pasos:

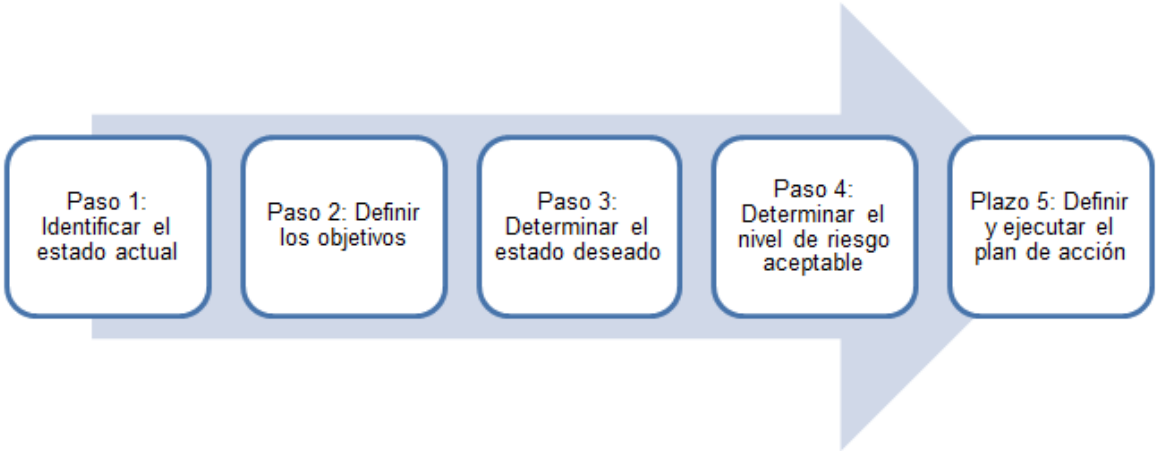

Ilustración 1. Pasos estratégicos para la adopción del Marco de Referencia.

7.1. Paso 1: Identificar el estado actual

A continuación se describen los objetivos, entradas, salidas y actividades del paso 1.

Objetivo:

Identificar el estado actual de capacidad o madurez del proceso de seguridad de la información con base en la clasificación de los activos de información.

Entradas:

- Inventario de activos de información.
- Metodología de valoración y clasificación de los activos de información.

Salidas:

- Activos de información clasificados con base en sensibilidad y criticidad.
- Meta establecida de seguridad de la información.
  Estado actual de seguridad de la información en la institución.

Actividades:

1. Determinar el estado actual de la seguridad de la información:

La alta dirección debe participar en la evaluación y análisis para determinar el estado actual del proceso de seguridad de la información. Generalmente el estado actual se determina luego de haber llevado a cabo una valoración análisis de la madurez o de la capacidad del proceso de seguridad de la información.

Para determinar el estado actual se pueden utilizar dos enfoques: a partir de un modelo de madurez o niveles de capacidad [7].

2. Identificar los activos de información.

Para llevar a cabo esta identificación, clasificación y valoración de los activos se utiliza el modelo que presenta el ISO/IEC 27002:2013.

3. Valorar los activos de información en función de su importancia para el negocio y del impacto que un incidente sobre el mismo puede causar a la institución.

Esta valoración se puede realizar en términos cuantitativos o cualitativos, por ejemplo:

- La valoración cuantitativa se basa en estimar el valor económico del activo. Esta valoración se puede efectuar realizando encuestas y entrevistas a los productores o responsables de custodiarlos activos. Con base en la información recolectada por estos medios se valora el activo. Los activos a los cuales se les puede realizar este tipo de valoración son, entre otros: sistemas de información, infraestructura y software.
- La valoración cualitativa se establece con base a una escala de valores, como por ejemplo del 0 al 10 o alto, medio, bajo. En esta valoración es necesario que existan criterios homogéneos de valoración que permitan comparar los activos. Para esta valoración debe utilizar como mínimo los criterios de confidencialidad, integridad y disponibilidad, los cuales obedecen a las características de la información. Por ejemplo, la valoración de una base de datos utilizando el criterios de confidencialidad definido anteriormente se puede llevar a cabo considerando el impacto que habría si un usuario no autorizado tuviera acceso a la base de datos y la modificara, afectando, en este caso, la confidencialidad de la información. En este caso la valoración se fundamentaría en el costo de recuperar los datos y el valor de las posibles sanciones por divulgación no autorizada.

4. Clasificar los activos de información con base en su criticidad y sensibilidad.

La metodología a utilizar para la clasificación la propone el MinTIC en su estrategia de Gobierno en Línea. [2] En dicha clasificación se plantean niveles de confidencialidad, integridad y criticidad que pueden aplicarse a cualquier institución del Estado.

7.2. Paso 2: Definir los objetivos

A continuación se describen los objetivos, entradas, salidas y actividades del paso 2:

Objetivos:

Dirigir los objetivos definidos para diseñar e implementar la Estrategia de Seguridad de la Información, para satisfacer los 6 objetivos de Gobierno de Seguridad de la Información que recomienda analizar y gestionar el Modelo de Negocio para la Seguridad de la Información de ISACA. [11]

Entradas:

- Plan estratégico institucional.
- Inventario de activos de información clasificados.
- Meta establecida de la seguridad de la información.
- Limitaciones de negocio o de recursos de TI que afecten el logro de los objetivos.
- Normatividad que aplique dentro de las instituciones por ejemplo: políticas de clasificación de privacidad de la información, ley de acceso y uso de información y sus decretos reglamentarios, reglamentación del Archivo General de la Nación sobre almacenamiento y protección de datos históricos, entre otros.
- Controles como sistemas de control de acceso, sistemas de detección de intrusos, entre otros.
- Contramedidas: estas hacen referencia a controles que se implementan en respuesta a una amenaza específica que se sabe que existe, pueden ser preventivas, de detección o correctivas, algunos ejemplos son: los sistemas de detección de intrusos para detectar intrusos en la red, encriptar o cifrar la información para evitar su intercepción; escaneo de virus, recompensas por delatar hackers.
- Sistemas de información y comunicaciones.

Salidas:

- Objetivos de la Estrategia de Seguridad de Información establecidos.

Actividades:

1. Definir los objetivos [11] de alineación estratégica.

El cumplimiento de estos objetivos debe permitir alinear los objetivos de la seguridad de la información con los objetivos de la institución para satisfacer:

- Requerimientos de seguridad de la información. Por ejemplo, controles de acceso a los dispositivos para garantizar la confidencialidad de la información de la institución.
- Ajustar las soluciones de seguridad a los procesos del negocio considerando: cultura, estilo de gobierno, tecnología y estructura de la organización de la institución.
- Inversión de seguridad de la información. Por ejemplo, presupuesto para la adquisición de herramientas para proteger la información de la institución contra ataques externos.

2. Definir los objetivos de gestión de riesgos:

El cumplimiento o logro de estos objetivos se traduce en la implementación de medidas apropiadas para mitigar los riesgos y reducir el posible impacto mediante:

- Entendimiento del perfil de amenaza, vulnerabilidad y riesgo de la organización.
- Entendimiento de la exposición al riesgo y las posibles consecuencias generadas por su materialización.
- Conciencia sobre las prioridades de la gestión de riesgos, con base en sus posibles consecuencias.
- Suficiente mitigación de riesgos para obtener consecuencias aceptables del riesgo residual.
- Aceptación / transferencia del riesgo a partir de un entendimiento de las posibles consecuencias por la materialización del mismo.
  Para realizar esta acción, se recomienda seguir los lineamientos planteados en la ISO/IEC 27005:2013 [8].

3. Definir los objetivos de entrega de valor:

El cumplimiento de estos objetivos debe permitir optimizar las inversiones en seguridad de la información en apoyo a los objetivos de la institución, teniendo en cuenta:

- Los requerimientos mínimos de seguridad proporcionales al riesgo y su impacto potencial.
- El esfuerzo debidamente priorizado y distribuido en áreas de mayor impacto y beneficio para el negocio.
- Las soluciones institucionalizadas y de uso general basadas en estándares.
- Una cultura continua, basada en el entendimiento de que la seguridad de la información es un proceso y no un incidente.

4. Definir los objetivos de gestión de recursos:

El cumplimiento de estos objetivos debe permitir utilizar el conocimiento y la infraestructura de seguridad de la información con eficiencia y efectividad para:

- Asegurar que los conocimientos sean captados y estén disponibles.
- Documentar los procesos y las prácticas de seguridad de la información.
- Desarrollar Arquitectura(s) de Seguridad para definir y utilizar los recursos de la infraestructura de manera eficiente.

5. Definir los objetivos de medición del desempeño:

El cumplimiento de estos objetivos debe permitir monitorear y reportar sobre los procesos de seguridad de la información, para garantizar que se alcancen los objetivos, entre los que se encuentran:

- Un conjunto de medidas definidas y acordadas debidamente alineadas con los objetivos estratégicos, que proporcionan la información necesaria para la toma de decisiones efectivas, en los niveles estratégicos, tácticos y operativos.
- Un proceso de medición que ayuda a identificar deficiencias y que proporciona retroalimentación sobre los avances hechos para resolver problemas.
- Aseguramiento independiente proporcionado por evaluaciones y auditorías externas.

Para la definición de los objetivos de medición puede utilizar como referencia COBIT 5.0 [8].

6. Definir los objetivos de integración:

El cumplimiento de estos objetivos permite integrar todos los factores relevantes de aseguramiento para garantizar que los procesos operen de acuerdo con lo planeado de principio a fin:

- Determinar todas las funciones organizacionales responsables del aseguramiento.
- Desarrollar relaciones formales con otras funciones de aseguramiento.
- Coordinar todas las funciones de aseguramiento para una seguridad más completa.
- Verificar que coincidan los roles y las responsabilidades entre las áreas de aseguramiento.
- Emplear un enfoque de sistemas para planificación, implementación y gestión de la seguridad de la información.

Para definir estos objetivos, se puede emplear el Modelo de Negocio para la Seguridad de la Información [11] de Isaca. En dicho documento se describe en detalle como cumplir con estos objetivos.

7.3. Paso 3: Determinar el estado deseado

A continuación se describen los objetivos, entradas, salidas y actividades del paso 3:

Objetivos:

Determinar el estado o nivel del estado deseado a alcanzar mediante la ejecución de la Estrategia de Seguridad de la Información en la organización, partiendo del estado o nivel actual de la institución.

Entradas:

- Objetivos de la Estrategia de Seguridad de la Información establecidos.
- Estado actual del proceso de seguridad de la información.
- Estándares internacionales y/o mejores prácticas como: ISO 27001:2013, ISO 27002:2013, CMMI, COBIT, ITIL, ISO/IEC 20000 y COSO.

Salidas:

- Estado deseado del proceso de seguridad de la información.

Actividades:

Identificar el nivel de madurez actual del proceso de seguridad de la información en la institución.

Este nivel de madurez se determina a través de la validación de los parámetros que presenta el modelo de madurez propuesto por COBIT 4.1, por ejemplo: verificando el cumplimiento los parámetros propuestos por COBIT 4.1 se sabrá en qué nivel de madurez se encuentra el proceso. Dentro de los elementos que se deben valorar para determinar si se cumple, o no se cumple con las características de madurez

predefinidas por COBIT, y sobre el cual se debe recopilar la respectiva evidencia que soporte su cumplimiento, se encuentran:

- Aceptación y apoyo de la alta dirección de la institución
- Alineamiento de la Estrategia de Seguridad de la Información con los objetivos institucionales
- Asignación clara de roles y responsabilidades
- Estructura organizacional que otorgue autoridad clara y apropiada a la gestión de seguridad de la información
- Identificación y clasificación de los activos de información, para determinar su criticidad y sensibilidad
- Controles efectivos
- Métricas de seguridad y procesos de monitoreo eficaces
- Procesos de cumplimiento, mediante el cual se debe garantizar el cumplir con la ley y con la normatividad de la institución
- Capacidad de respuesta ante incidentes y emergencias de seguridad
- Planes de continuidad del negocio y recuperación de desastres probados
- Procesos de gestión de cambio que cuentan con aprobación de seguridad de la información
- Riesgos identificados, evaluados, comunicados y gestionados
- Conciencia sobre la necesidad de la seguridad de la información

1. Definir el estado deseado del proceso de seguridad de la información dentro de la institución en términos cualitativos de atributos, características y resultados.

Existen varios enfoques para ayudar a determinar el nivel del "estado actual" y el nivel del "estado deseado" a alcanzar, entre ellos:

- Aplicar un Modelo de Madurez de la Capacidad, como el que ofrece COBIT® 4.1 para saber en dónde se encuentra el proceso de seguridad de la información y a dónde se quiere llegar
- Aplicar el Modelo de Capacidad como el que ofrece COBIT® 5, para saber en dónde se encuentra el proceso de seguridad de la información y a donde se quiere llegar.

2. Identificar el nivel de madurez deseado:

El dueño del proceso en unión con la alta gerencia debe determinar el nivel de madurez deseado, en el cual se debería encontrar el proceso para que cumpla con sus objetivos y satisfaga las necesidades de la institución.

7.4. Paso 4: Determinar el nivel de riesgo aceptable

A continuación se describen los objetivos, entradas, salidas y actividades del paso 4:

Objetivos:

Determinar el nivel de riesgo aceptable para la seguridad de la información, a ser considerado en la Estrategia de Seguridad de la Información con base en el apetito de riesgo de la organización.

Entradas:

- Objetivos de la Estrategia de Seguridad de la Información establecidos
- Estado actual del proceso de seguridad de la información
- Estado deseado del proceso de seguridad de la información
- Apetito de riesgo de la organización. Para esto es importante que cada la alta dirección de cada institución identifique y formalice su apetito de riesgo. Este apetito de riesgo se refiere al riesgo que una institución está dispuesta a correr para lograr sus objetivos
- Metodología de gestión de riesgos [4]

Salidas:

- Nivel de riesgo aceptable
- Mapa de riesgos de TI
- Estrategia de Seguridad de la Información actualizada

Actividades:

1. Identificar el apetito de riesgo de la institución

Es decir, que es lo que la alta dirección considera un riesgo aceptable. El apetito de riesgo es determinado por la institución con base en el riesgo que está dispuesta a correr por obtener un beneficio antes que la utilidad sea menor que la pérdida.

2. Determinar el nivel de riesgo aceptable para la seguridad de la información.

Con base en este nivel de riesgo se deberán gestionar los riesgos relacionados con la seguridad de la información.

3. Aplicar una metodología de gestión de riesgo a nivel de TI en la institución.

Para identificar sus riesgos y promover su tratamiento para evitar, en lo posible, que sus riesgos se materialicen. Estas metodologías pueden ser ISO/IEC 27005:2013, Octave [12], Magerit [13], ISO/IEC 31000, NTC5254.

4. Enfocar la Estrategia de Seguridad a la gestión de los riesgos críticos encontrados.

7.5. Paso 5: Definir y ejecutar el plan de acción

A continuación se describen los objetivos, entradas, salidas y actividades del paso 5:

Objetivos:

Establecer el plan de acción para alcanzar el estado deseado de la Estrategia de Seguridad de la Información, incluyendo personas, tecnologías y procesos, entre otros recursos [5].

Entradas:

- Objetivos de la Estrategia de Seguridad de la Información establecidos
- Estado actual del proceso de seguridad de la información
- Estado deseado del proceso de seguridad de la información
- Activos de Información:
  - Políticas
  - Estándares
  - Procedimientos
  - Directrices
  - Arquitectura (s)
  - Controles físicos, tecnológicos y de procedimientos
  - Tecnologías
  - Roles y responsabilidades
  - Proveedores de servicios externos
  - Instalaciones
  - Elementos de seguridad de la información
  - Seguridad en el entorno
  - Contramedidas
  - Defensa en capas
  - Seguridad del personal

- Conciencia y formación
- Auditorías
- Cumplimiento
- Evaluación de amenazas
- Análisis de vulnerabilidades
- Evaluación de riesgos
- Análisis de impacto del negocio

Salidas:

- Hoja de ruta de correspondiente al plan de acción para la implementación de la seguridad de la información, en la cual se priorizarán las iniciativas que se deben llevar a cabo para cerrar la brecha y alcanzar el estado deseado.
- Plan de Uso y Apropiación de la Estrategia en Seguridad de la Información.
- Métricas (BSC) y mecanismos de monitoreo de la Estrategia de Seguridad de la Información.

Actividades:

1. Estimar para cada una de las acciones definidas en la Estrategia.

Los recursos requeridos y el costo para desarrollarla. Para realizar la cuantificación se puede apoyar en las guías y anexos vigentes del modelo de seguridad y privacidad de la información.

2. Identificar limitaciones:

- Legales: leyes y regulaciones. Importante identificar todas las leyes colombianas, así como posible legislación extranjera que se deba cumplir gracias a acuerdos internacionales, como podría ser normatividad de la ONU o de la OEA.
- Físicas: limitaciones de capacidad, espacio y entorno.
- Éticas: apropiadas, razonables y habituales.
- Culturales: tanto dentro, como fuera de la organización.
- De costos: tiempo y dinero.

- Personales: resistencia al cambio y resentimiento contra nuevas limitaciones.
- De estructura organizacional: cómo se toman las decisiones, quién lo hace.
- De recursos: de capital, tecnología y humanos.
- De capacidades: conocimientos, habilidades y conocimientos especializados.
- De tolerancia al riesgo: ventana de oportunidad y cumplimiento forzoso.

3. Habiendo identificado el "estado actual" y el "estado deseado" del proceso de seguridad de la información.

Se debe analizar la brecha existente entre estos dos estados, identificando la brecha a cerrar con la implementación de la estrategia de seguridad de la información. Para realizar este análisis, se puede considerar lo definido por COBIT en sus versiones 4.1 o 5.0.

4. Establecer planes de acción y proyectos para cerrar la brecha y llegar al estado deseado.

Dentro de estos planes debe considerarse la elaboración, si se requiere, de políticas de seguridad de la información incluyendo cada uno de sus dominios y sus principales subdivisiones del ISO/IEC 27001:2013 o el ISO/IEC 27002:2013 [8]. Es probable que cada política tenga varios estándares de apoyo que, generalmente, se dividirán en dominios de seguridad. Adicionalmente, como resultado de la evaluación de la

5. Elaborar estándares de seguridad de la información que soporten la política.

Para elaborar los estándares, también se puede utilizar el ISO/IEC 27002:2013.

6. Definir y ejecutar un programa continuo de sensibilización y capacitación en seguridad, que permita implementar y adoptar por todos los miembros de la institución una Estrategia de Seguridad de la Información eficaz.

Cuando se emita una nueva política de seguridad de la información o se modifique otra, debe capacitarse a todo el personal implicado para que puedan ver la relación entre las políticas y los estándares, y sepan qué deben hacer para cumplirlos.

Establecer métodos de monitoreo y medición del progreso y el logro de las etapas importantes de la ejecución del plan de acción, para implementar la Estrategia. Uno de los métodos más utilizados es emplear un BSC para dar seguimiento a los indicadores de forma continua.

8. ANEXO. ACTIVOS DE INFORMACIÓN (DEFINICIONES)

Amenazas: Hecho que puede facilitar la materialización de un riesgo.

Análisis de impacto del negocio: Subproceso mediante el cual se determinan y entienden los procesos críticos que son esenciales para la continuidad de servicios y se calcula su posible impacto con el fin de priorizar su ciclo de recuperación. Es una fase del plan de continuidad del negocio.

Análisis de vulnerabilidades: Metodología mediante la cual se evalúan los sistemas y servicios de TI, en una organización y se verifica la existencia de vulnerabilidades (debilidades o faltas de control). Las vulnerabilidades son puntos débiles del sistema que permiten que un atacante comprometa la integridad, disponibilidad o confidencialidad del mismo.

Arquitectura(s): Es el diseño de los componentes lógicos y físicos de cómputo y las relaciones entre éstos. La Arquitectura define el hardware, software, métodos de acceso y protocolos usados a través del sistema. También se define como un marco de trabajo y un conjunto de lineamientos para construir un nuevo sistema.

Auditorías: Proceso mediante el cual se lleva a cabo una evaluación de riesgos y controles de un objetivo componente general o particular.

Contramedidas: Controles específicos para riesgos específicos.

Controles: Es un mecanismo preventivo, detector o correctivo adoptado por la administración de una dependencia o institución que permite la prevención, detección y corrección de desviaciones, ineficiencias o incongruencias en el curso de la formulación, instrumentación, ejecución y evaluación de las acciones, con el propósito de procurar el cumplimiento de la normatividad que las rige, y las estrategias, políticas, objetivos, metas y asignación de recursos.

Directrices: Fijan las condiciones generales de actuación. La directriz tiene carácter normativo, por lo que debe ser general en su contenido y ámbito. Toman las políticas y las transforman en acciones.

Estándares: Reglas que especifican una acción o respuesta que se debe seguir en una situación determinada. Son obligatorios y su misión es hacer cumplir las políticas, por

ende, se diseñan para promover la implementación de las políticas de alto nivel de la organización o de TI.

Estructuras organizacionales: Estructura mediante la cual se subdividen las áreas de negocio de una empresa y se implementan buenas prácticas de segregación de responsabilidades mecanismos de escalamiento y criterios de autoridad.

Instalaciones: Sitio físico donde se procesa y almacena información.

Políticas: Mecanismos a través de los cuales se indica o transmite la intención de la alta gerencia respecto a la operación y/o gestión de la organización. Son pautas generales que se dan a los funcionarios para que puedan tomar decisiones, tanto en el presente, como en el futuro.

Procedimientos: Pasos que deben ser seguidos por un área o dependencia de TI, para implementar políticas, procesos, estándares, sistemas específicos, servicios, mejores prácticas y guías, entre otros.

Proveedores de servicios externos: Personas u organizaciones que prestan servicios a una institución.

Riesgos: Pérdida potencial por daños, interrupción, alteración o fallas derivadas del uso o dependencia en el hardware, software, sistemas, aplicaciones, redes y cualquier otro canal de distribución de Información que el Instituto dispone para prestar sus servicios. Es la probabilidad de ocurrencia de un evento.

9. REFERENCIAS

[1] K. Andrews. The Concept of Corporate Strategy. 2nd Edition. [Online]. Disponible en: http://www.amazon.com/Concept-Corporate-Strategy-Kenneth-Andrews/dp/0870949837, [Último acceso: 30 de junio de 2014].

[2] Ministerio de Tecnologías de la Información y las Comunicaciones. (2011). "Anexo 7: Metodología de Clasificación de Activos - Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea".

[3] ISACA (2014). Certified Information Security Manager (CISM) Review Manual. ISBN 978-60420-215-1. [Online]. Disponible en: https://www.isaca.org/bookstore/Pages/Product-Detail.aspx?Product_code=CM14, [Último acceso: 10 de julio de 2014].

[4] Instituto Colombiano de Normas Técnicas y Certificación - ICONTEC (2011) NTC-31000. Metodología de Gestión de Riesgos.

[5] ITGI. (2008). Information Security Governance: Guidance for Information Security Managers. [Online]. Disponible en: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Information-Security-Governance-Guidance-for-Information-Security-Managers.aspx, [Último acceso: 14 de julio de 2014].

[6] ISACA. COBIT© 5. A business framework for the governance and management of enterprise IT. ISBN: 978-60420-237-3. 2012.

[7] ISO/IEC 27002:2013. Information Technology – Security Techniques – Code of Practices for Information Security Controls.

[8] ISO/IEC 27005:2013. Information Technology – Security Techniques – Information Security Risk Management.

[9] ISACA, (2007) Val IT. Enterprise Value: Governance of IT Investments – The Val IT Framework 2.0. ISBN: 978-1-60420-066-9.

[10] CONPES 3701, (2011). Lineamientos de políticas para Ciberseguridad y Ciberdefensa.

[11] ISACA. The Business Model for Information Security, (2010). ISBN: 978-1-60420-154-3.

[12] OCTAVE, Operationally Critical Threat, Asset and Vulnerability Evaluation. Software Engineering Institute, 2005.

[13] MAGERIT, 2013. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Gobierno de España. NIPO: 630-12-171-8.