UNIVERSIDAD DON BOSCO

VICERRECTORÍA DE ESTUDIOS DE POSTGRADO

TRABAJO DE GRADUACIÓN

"Propuesta de un marco genérico para implementar modelos de madurez de seguridad de la información"

PARA OPTAR AL GRADO DE:

MAESTRO EN SEGURIDAD Y GESTION DE RIESGOS INFORMATICOS

ASESOR:

DOCTOR CARLOS RAUDALES

PRESENTADO POR:

ROSA MARÍA MONGE ALVARENGA

ELMER ARTURO CARBALLO RUÍZ

ROBERTO MAURICIO RODRÍGUEZ MARTÍNEZ

Antiguo Cuscatlán, La Libertad, El Salvador, Centroamérica

JULIO 2015

Contenido

CAPITULO 1: EL PROBLEMA DE INVESTIGACIÓN

1.1 Identificación del Problema

En la medida que las organizaciones se concientizan de la necesidad de evaluar el presente estado de la seguridad de la información, el impacto que ocasiona la pérdida de información e imagen corporativa, surge la vital importancia de utilizar modelos de madurez que les permitan conocer su estado actual y las vulnerabilidades que poseen como elementos fundamentales para realizar un plan de mejora. Las organizaciones necesitan cuestionarse que es lo que están realizando para garantizar la seguridad de la información que gestiona, la cual se convierte en un activo crítico para el seguimiento de sus operaciones.

La importancia de los modelos de madurez es que pueden permitir la medición del progreso de un programa de seguridad y/o un sistema de gestión de seguridad de la información, ya que permite medir cosas significativas y la progresión que llevan hacia un objetivo. Los modelos de madurez (Arbeláez, 2008) permiten establecer un orden claro, discreto y absoluto; definiendo niveles o etapas de madurez que facilitan conocer la evolución de la organización.

Los pocos modelos de madurez orientados a la seguridad deberían permitir medir donde se está actualmente, facilitando proyectarse hacia donde se debe estar acorde a la estrategia competitiva y apetito de riesgo de la organización. Sin embargo según la investigación realizada por Luis Enrique Sánchez (Sánchez, Villafranca, Fernández-Medina, & Piattini, 2009) en numerosas fuentes bibliográficas se detecta y resalta la dificultad que supone para las pequeñas y medianas empresas la utilización de las metodologías y modelos de madurez por el grado de compresión del proceso a seguir y el alto costo. Se han desarrollado algunos modelos de madurez para la seguridad de la información, pero la mayoría se vuelven complejos en su implementación; otros modelos si establecen una guía pero es difícil de implementar por su alto costo o requiere de personal experto que lo implementen.

Según un artículo publicado por (Elizabeth Pérez Mergarejo, 2013) la información disponible sobre los modelos de madurez es escaza y en el contexto Latinoamericano la aplicación de estos es incipiente. Según Mergarejo (Elizabeth Pérez Mergarejo, 2013) para algunos modelos de madurez su aplicación se dificulta debido al desconocimiento sobre el tema y la insuficiente preparación de las personas implicadas en su aplicación (alta dirección, responsables de procesos, etc.).

En el artículo “Towards a new Maturity Model for Information Security Management” (MATRANE, TALEA, & OKAR, 2014) se plantea que a medida la información de la seguridad se ha convertido en un rol importante para soportar las actividades de las organizaciones se necesita un estándar o comparaciones. Se han creado numerosos estándares que guían la seguridad de la información sin embargo no son bien adoptadas debido a diferentes razones.

Todo esto lleva a preguntarse diferentes aspectos, entre los cuales uno fundamental es porque razón las organizaciones no implementan modelos de madurez de la seguridad de la información que le permitan medir su nivel de seguridad, esto podría ser por algunas de las siguientes razones:

1. Desconocimiento sobre la existencia de modelos que miden la madurez de la seguridad de la información.
2. Falta de conciencia del impacto sobre las organizaciones al no tener un modelo de madurez que mida el grado de seguridad de la información en sus organizaciones.
3. Complejidad que presenta el proceso o metodología al implementar un modelo de madurez de la seguridad de la información.
4. Necesidad de personal con cierto grado de especialización y conocimiento del modelo de madurez para poder implementarse.
5. Bajo presupuesto financiero y recursos en las organizaciones para poder implementar un modelo de madurez.
6. Una guía práctica compleja o incompleta sobre cómo implementar un modelo de madurez de la seguridad de la información.
7. Ausencia de objetivos estratégicos que contemplen un plan que evalué la seguridad de la información.

Lo que lleva a plantearse de manera esquematizada la siguiente problemática (figura 1):

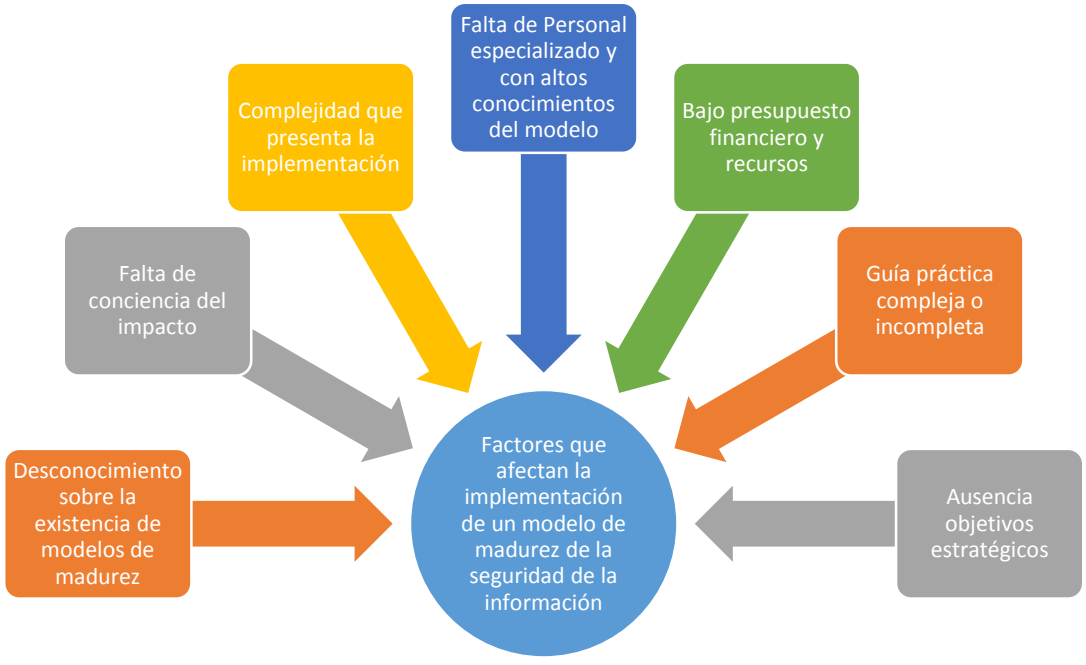


Figura 1. Planteamiento del problema

1.2 Formulación del Problema

¿Cuáles son los factores que afectan la falta de un marco genérico para la implementación de un modelo de madurez que permita medir la seguridad de la información para una organización?

1.3 Objetivos

1.3.1 General

- Proponer un marco de trabajo genérico que permita medir la madurez de la seguridad de la información para la implementación de un modelo facilitando su uso y adaptabilidad al tipo de organización.

1.3.2 Específicos

- Seleccionar la información de fuentes primarias y secundarias de algunos marcos, modelos y/o metodologías de madurez aplicados a la seguridad de la información que sirvan de base para la construcción de un marco de trabajo.
- Identificar de qué manera los modelos de seguridad de la información existentes son adaptables, comprensibles y factibles de implementar en organizaciones sin importar su rubro y tamaño.
- Diseñar un marco de trabajo genérico que permita la implementación de un modelo de madurez que mida la seguridad de la información en una organización.

1.4 Justificación de la Investigación

En la actualidad las organizaciones se ven preocupadas y alertadas por el aumento de ataques cibernéticos como es el robo de información confidencial, afectar la reputación e imagen corporativa, la integridad de la información, accesos no autorizados a los datos, esto ha provocado una clara necesidad de proteger los activos de la organización como elemento clave que brinde confianza necesaria a los clientes, usuarios y proveedores sobre las relaciones o manejos de su información.

Cada vez más organizaciones están descubriendo las ventajas y la importancia que conlleva la seguridad de la información, están apostando por los beneficios que otorga la gestión de la seguridad de la información, en primer lugar se ve beneficiado la imagen y credibilidad de la organización, posteriormente una adecuada gestión de seguridad puede producir la reducción de pérdidas que tengan un alto impacto negativo para la organización y les permite obtener nuevas oportunidades de inversión. Además que la seguridad se ha convertido en un apoyo al logro de los objetivos de negocio y estratégicos.

Garantizar la seguridad de la información se ha vuelto una de las principales tareas dentro de las organizaciones, ya que sus clientes, proveedores e interesados están exigiendo que se aseguren sus activos y no se ponga en riesgos sus inversiones por lo que necesitan herramientas que permitan satisfacer la necesidad de verificar el estado de la seguridad; debido a esto se ha considerado que las empresas de la región deben contar con un marco de trabajo genérico que les permita facilitar y conocer el nivel de madurez en el que se encuentra la Organización con respecto a la Seguridad de la Información.

Este estudio pretende mostrar una alternativa de un marco de trabajo que facilite su compresión e implementación para medir la seguridad de tal forma que posea fases y pasos que de manera sencilla y comprensible logre adaptarse. Esta investigación proporcionará un modelo como propuesta y que sirva como instrumento para medir la seguridad de la información en una organización. El resultado de esta investigación permitirá dar un modelo valorizado por expertos de seguridad que brinde los beneficios propuestos y que permita medir la madurez de la organización en términos de la información, intentando su facilidad práctica y adaptabilidad al contexto.

Esta propuesta es un marco de trabajo genérico para implementar un modelo de madurez de la Seguridad de la información. Esta será una herramienta que impulse a las organizaciones salvadoreñas a involucrarse en la gestión de la seguridad de la información. Además que facilite su implementación, sea de fácil compresión y se adapte al tipo de organización sin importar su rubro o tamaño.

1.5 Alcance

El diseño de un marco de trabajo que permita la implementación de un modelo de madurez de seguridad de la información que sea adaptable a cualquier tipo de organización salvadoreña o de la región centroamericana, sin importar su tamaño. Esta propuesta de marco genérico se desarrollará solo hasta la fase de diseño y valoración por expertos, debido a que se cuenta con una limitación en el tiempo de desarrollo por lo que la fase de implementación deberá considerarse para trabajos futuros.

Los entregables de la propuesta son los siguientes:

- Un informe que contenga el estudio realizado para la propuesta del marco de trabajo genérico que permita medir la madurez de la seguridad de la información.
- Un artículo que contendrá de manera resumida la propuesta del marco de trabajo genérico que permita medir la madurez de la seguridad de la información.

CAPITULO 2: MARCO TEORICO

2.1 Estado del Arte

Con la creciente dependencia que la sociedad de la información tiene de las Tecnologías de la Información (TI), la necesidad de proteger la información tiene cada vez mayor importancia para las empresas, según Luis Sánchez (Sánchez, Villafranca, Fernández-Medina, & Piattini, 2009). De esta manera, la demanda de productos, sistemas y servicios para gestionar y mantener la información es creciente, y no es suficiente con realizar unos controles de seguridad superficiales o específicamente de TI Es necesario aplicar un enfoque detallado y amplio para evaluar y mejorar la seguridad de los servicios, productos y también de los procesos o dominios que se llevan a cabo en el contexto de las TI.

En este contexto, surgen los Sistemas de Gestión de la Seguridad de la Información (SGSI), que tienen una gran importancia para la estabilidad de los sistemas de información de las compañías. Un SGSI se puede definir como un sistema de gestión usado para establecer y mantener un entorno seguro de la información. El objetivo principal de los SGSIs es afrontar, la puesta en práctica y el mantenimiento de los procesos y los procedimientos necesarios para manejar la seguridad de las tecnologías de la información, de acuerdo a Jan Eloff (Jan Eloff, 2003).

A pesar de que existen varios estándares y recomendaciones que abordan la gestión de la seguridad, así como algún modelo de madurez para la seguridad, en la práctica estos estándares y recomendaciones son muy difíciles de implantar, y requieren una inversión demasiado alta, que la mayoría de las empresas no puede asumir según Luis Enrique Sánchez (Sánchez, Villafranca, Fernández-Medina, & Piattini, 2009), y de acuerdo con lo que plantea Elizabeth Mergarejo (Elizabeth Pérez Mergarejo, 2013) en su estudio donde describe que además de que los modelos de madurez son costosos, no disponen de procedimientos para su implementación.

Un modelo de madurez es un mapa que guía a la organización en la implementación de buenas prácticas, ofreciendo un punto de partida. Describe un camino de mejoramiento evolutivo, desde los procesos inconsistentes hasta los más maduros de la organización según la definición que plantea Mergarejo (Elizabeth Pérez Mergarejo, 2013). Permite evaluar el estado de desarrollo de una organización o proceso de negocio, trazar claramente estrategias de mejoras para alcanzar los objetivos previstos e identificar las áreas donde la organización debe enfocarse para mejorar.

Los Modelos de Madurez, son muy comunes en las organizaciones de TI e industria del software, ayudan a una organización a evaluar sus métodos y procedimientos de acuerdo con criterios de gestión. Los ejemplos más conocidos de Modelos de Madurez son los desarrollados por el Instituto de Ingeniería de Software conocido por sus siglas en inglés SEI (Software Engineering Institute) de la Universidad Carnegie Mellon, de acuerdo a Juan Manuel Gers (Juan Manuel Gers & José Enar Muñoz Narváez, 2014). Los modelos de madurez (Elizabeth Pérez Mergarejo, 2013) constituyen una evolución de las prácticas para gestionar la calidad. Fueron concebidos inicialmente para la industria del software y en la actualidad el área de aplicación es

muy diversa. Se pueden encontrar aplicaciones en: el desarrollo de software, la gestión de proyectos, la gestión del conocimiento, el desarrollo de los procesos, la Gestión de Procesos de Negocio o en inglés *Business Process Management* (BPM).

De acuerdo a Mergarejo, entre los usos más comunes de los modelos de madurez se encuentran: realizar benchmarking, evaluar riesgos de desarrollo e implementación de aplicaciones empresariales y guiar programas de mejoras para procesos de negocio. Entre los modelos de madurez más divulgados y complejos por su estructura y aplicación se pueden citar: Capability Maturity Model (CMM), Capability Maturity Model Integration (CMMI) del Departamento de Defensa de los Estados Unidos y del SEI, en un principio concebidos para la evaluación de la capacidad de las organizaciones desarrolladoras de proyectos de software. Según un informe de Saavedra (Saavedra, 2006) luego de varias décadas de no obtener resultados satisfactorios con las nuevas tecnologías y metodologías de software, el sector empresarial y gubernamental, se da cuenta que sufre de incapacidad al manejar sus procesos de software. Por esos años, los proyectos generalmente padecían de demoras excesivas así como duplicación del presupuesto acordado. En estas circunstancias era imposible apreciar las ventajas que podían proveer las nuevas metodologías y métodos. Es por eso que en noviembre de 1986, el SEI, con la asistencia de Mitre Corporation, comenzó a desarrollar un framework de madurez de proceso, el que asistiría a las organizaciones a mejorar su proceso de Software. En septiembre de 1987, el SEI presenta una breve descripción en el informe de Humphrey (Humphrey, 1987) el cual fuera posteriormente profundizado en el libro de Humphrey "Managing the Software Process" (Humphrey, Managing the Software Process, 1989). Dos métodos, "Aseguración de procesos de software" y "Cuestionario de madurez y evaluación" (Schulz, 1987) fueron desarrollados para aproximar la madurez de procesos de Software. Luego de experimentar por cuatro años el framework de Madurez de Procesos y una versión preliminar del cuestionario de madurez, el SEI evolucionó el mencionado framework a lo que es el Modelo de madurez de capacidad (o Capability Maturity Model for Software) (Paulk, Curtis, Chrissis, & Weber, 1993). El CMM presenta un conjunto de prácticas recomendadas dentro de varias áreas de procesos claves que han demostrado realzar la capacidad de proceso del Software. Está basado en el conocimiento adquirido por mejoras en el proceso de software y extensiva retroalimentación (feedback) tanto de la industria como del gobierno.

Este modelo provee a las organizaciones de Software dar una guía de cómo controlar los procesos para desarrollar y mantener software además de cómo evolucionar en una cultura de ingeniería de Software y administración de excelencia. Fue diseñado para guiar a las organizaciones a seleccionar estrategias para mejorar procesos determinando la madurez actual del proceso e identificando algunos inconvenientes críticos en la calidad de Software y mejora del proceso. Concentrándose en un conjunto de actividades y trabajando agresivamente para lograrlas, una organización puede mejorar la amplitud de proceso permitiendo logros continuos y capacidad perdurable.

Capability Maturity Model (CMM) *(Paulk, Curtis, Chrissis, & Weber, 1993)*

A partir de noviembre de 1986 el SEI, a requerimiento del Gobierno Federal de los Estados Unidos de América (en particular del Departamento de Defensa, en sus siglas DoD), desarrolló una primera definición de un modelo de madurez de procesos en el desarrollo de software, que se publicó en septiembre de 1987. Este trabajo evolucionó al modelo CMM o SW-CMM (CMM for Software). Este modelo establece un conjunto de prácticas o procesos claves agrupados en Áreas Clave de Proceso (KPA - Key Process Area). Para cada área de proceso define un conjunto de buenas prácticas que habrán de ser:

- Definidas en un procedimiento documentado
- Provistas (la organización) de los medios y formación necesarios
- Ejecutadas de un modo sistemático, universal y uniforme (institucionalizadas)
- Medidas
- Verificadas

A su vez estas Áreas de Proceso se agrupan en cinco "niveles de madurez", de modo que una organización que tenga institucionalizadas todas las prácticas incluidas en un nivel y sus inferiores, se considera que ha alcanzado ese nivel de madurez.

Los niveles son:

0 - Inexistente. Las Organizaciones carecen completamente de cualquier proceso reconocible e incluso se desconoce la existencia de un problema a resolver.

1 - Inicial. Las organizaciones en este nivel no disponen de un ambiente estable para el desarrollo y mantenimiento de software. Aunque se utilicen técnicas correctas de ingeniería, los esfuerzos se ven minados por falta de planificación. El éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y por consiguiente un aumento en los costos. El resultado de los proyectos es impredecible.

2 - Repetible. En este nivel las organizaciones disponen de unas prácticas institucionalizadas de gestión de proyectos, existen unas métricas básicas y un razonable seguimiento de la calidad. La relación con subcontratistas y clientes está gestionada sistemáticamente.

3 - Definido. Además de una buena gestión de proyectos, a este nivel las organizaciones disponen de correctos procedimientos de coordinación entre grupos, formación del personal, técnicas de ingeniería más detallada y un nivel más avanzado de métricas en los procesos. Se implementan técnicas de revisión por pares (peer reviews).

4 - Gestionado. Se caracteriza porque las organizaciones disponen de un conjunto de métricas significativas de calidad y productividad, que se usan de modo sistemático para la toma de decisiones y la gestión de riesgos. El software resultante es de alta calidad.

5 - Optimizado. La organización completa está volcada en la mejora continua de los procesos. Se hace uso intensivo de las métricas y se gestiona el proceso de innovación.

Así es como el modelo CMM establece una medida del progreso, conforme al avance en niveles de madurez. Cada nivel a su vez cuenta con un número de áreas de proceso que deben

lograrse. El alcanzar estas áreas o estadios se detecta mediante la satisfacción o insatisfacción de varias metas claras y cuantificables. Con la excepción del primer nivel, cada uno de los restantes Niveles de Madurez está compuesto por un cierto número de Áreas Claves de Proceso, conocidas a través de la documentación del CMM por sus siglas del inglés: KPA. Cada KPA identifica un conjunto de actividades y prácticas interrelacionadas, las cuales cuando son realizadas en forma colectiva permiten alcanzar las metas fundamentales del proceso. Las KPAs pueden clasificarse en 3 tipos de proceso: Gestión, Organizacional e Ingeniería.

Las prácticas que deben ser realizadas por cada Área Clave de Proceso están organizadas en 5 Características Comunes, las cuales constituyen propiedades que indican si la implementación y la institucionalización de un proceso clave es efectivo, repetible y duradero. Estas 5 características son:

i. Compromiso de la realización
ii. La capacidad de realización
iii. Las actividades realizadas
iv. Las mediciones y el análisis
v. La verificación de la implementación.

Las organizaciones que utilizan CMM para mejorar sus procesos disponen de una guía útil para orientar sus esfuerzos. Además, el SEI proporciona formación a evaluadores certificados (Lead Assesors) capacitados para evaluar y certificar el nivel CMM en el que se encuentra una organización. Esta certificación es requerida por el Departamento de Defensa de los Estados Unidos, pero también es utilizada por multitud de organizaciones de todo el mundo para valorar a sus subcontratistas de software.

Se considera típico que una organización dedique unos 18 meses para progresar un nivel, aunque algunas consiguen mejorarlo. En cualquier caso requiere un amplio esfuerzo y un compromiso intenso de la dirección. Como consecuencia, muchas organizaciones que realizan funciones de desarrollo de software o, en general, outsourcing de procesos de software, adoptan el modelo CMM y se certifican en alguno de sus niveles. Esto explica que uno de los países en el que más organizaciones certificadas existen sea en India, donde han florecido los desarrollos de software que trabajan para clientes estadounidenses y europeos.

Capability Maturity Model Integration (CMMI) (Carnegie Mellon University , 2010)

El modelo CMMI desarrollado por el SEI de la Universidad Carnegie Mellon, es un modelo de procesos que permite identificar el nivel de madurez de una organización basándose en la capacidad de sus procesos, con el fin de facilitar y simplificar la adopción de varios modelos de forma simultánea, tales como:

- CMM-SW (*CMM for Software*)
- SE-CMM (*Systems Engineering Capability Maturity Model*)
- IPD-CMM *(Integrated Product Development*)

El modelo CMMI tiene dos tipos de representaciones: continua y escalonada. Estas dos representaciones son equivalentes y las organizaciones pueden optar por la mejor que se adapte a sus características y prioridades de mejora. La representación continua tiene como objetivo el nivel de capacidad de cada una de las áreas de proceso del modelo, mientras que la representación escalonada evalúa la madurez de la organización basándose en etapas definidas.

La representación continua está conformada por 6 niveles de capacidad, los cuales son:

i. Nivel 0. - Incompleto: El proceso no se realiza, o no se consiguen sus objetivos.
ii. Nivel 1. - Ejecutado: El proceso se ejecuta y se logra su objetivo.
iii. Nivel 2. - Gestionado: Además de ejecutarse, el proceso se planifica, se revisa y se evalúa para comprobar que cumple los requisitos.
iv. Nivel 3. - Definido: Además de ser un proceso "gestionado" se ajusta a la política de procesos que existe en la organización, alineada con las directivas de la empresa.
v. Nivel 4. - Cuantitativamente gestionado: Además de ser un proceso definido, se controla utilizando técnicas cuantitativas.
vi. Nivel 5. - En optimización: Además de ser un proceso cuantitativamente gestionado, de forma sistemática se revisa y modifica para adaptarlo a los objetivos del negocio.

La representación escalonada permite ubicar en qué lugar se encuentra la organización en uno de los 5 niveles de madurez en los que está distribuido el modelo. Estos niveles son:

- Nivel 1: Inicial. Los resultados de calidad obtenidos en el proceso de software son impredecibles, sin control, reactivo y son consecuencia de las personas y de las herramientas que emplean. Este nivel no depende de los procesos previamente definidos por la organización, ya que estos no existen o no son utilizados.
- Nivel 2: Gestionado. Se considera un nivel 2 de madurez cuando se llevan a cabo prácticas básicas de gestión de proyectos (costos, cronograma, funcionalidad), de gestión de requisitos, control de versiones y de los trabajos realizados por subcontratistas. Los equipos de los proyectos pueden aprovechar las prácticas realizadas para aplicarlas en nuevos proyectos.
- Nivel 3: Definido. Los procesos comunes para desarrollo y mantenimiento del software están documentados de manera suficiente en una biblioteca accesible a los equipos de desarrollo. Las personas han recibido la formación necesaria para comprender los procesos.
- Nivel 4: Gestionado cuantitativamente. La organización mide la calidad del producto y del proceso de forma cuantitativa con base en métricas establecidas. La capacidad de los procesos empleados es previsible y el sistema de medición permite detectar si las variaciones de capacidad exceden los rangos aceptables para adoptar medidas correctivas.
- Nivel 5: En optimización. La mejora continua de los procesos afecta a toda la organización, que cuenta con medios para identificar las debilidades y reforzar la prevención de defectos. Se analizan de forma sistemática datos relativos a la eficacia de los procesos de software para analizar el costo y el beneficio de las adaptaciones y las mejoras. Se evalúan e implementan tecnologías innovadoras, buscando la mejora continua de los procesos.

Modelo de Madurez de Capacidades en la Ingeniería de Seguridad de Sistemas (SSE-CMM) (Carnegie Mellon University, 1999)

El System Security Engineering Capability Maturity Model (SSE-CMM)o Modelo de Madurez de Capacidades en la Ingeniería de Seguridad de Sistemas es un modelo derivado del CMM y que describe las características esenciales de los procesos que deben existir en una organización para asegurar una buena seguridad de sistemas. Ha sido desarrollado por la "International Systems Security Engineering Association (ISSEA)", organización sin ánimo de lucro patrocinada por un buen número de compañías dedicadas a la seguridad de sistemas. Nació a partir de 1993 bajo los auspicios de la Agencia Nacional de Seguridad (NSA) de los E.U.A., con la participación de numerosas compañías de los sectores de tecnologías de la información, seguridad y defensa.

Pretende servir como:

- Herramienta para que las organizaciones evalúen las prácticas de ingeniería de seguridad y definan mejoras a las mismas.
- Mecanismo estándar para que los clientes puedan evaluar la capacidad de los proveedores de ingeniería de seguridad.
- Base para la organización de un mecanismo de evaluación y certificación.

A diferencia del CMM original, las áreas de proceso no están agrupadas en función de los niveles de madurez, sino que define 22 áreas para cada una de las cuales se puede alcanzar un nivel en función del cumplimiento de unas "características comunes". Existen 11 áreas de procesos de ingeniería y otras 11 dedicadas a la gestión de proyectos y organización. El método de evaluación se denomina SSAM (SSE-CMM Appraisal Method).

2.2 Antecedentes de la Investigación

Existen algunos modelos de madurez cuyo dominio de aplicación es la seguridad de la información. En la revisión bibliográfica se analizaron una variedad de documentos, los aportes obtenidos de los modelos de madurez, metodologías, investigaciones y desarrollos estudiados ofrecen información valiosa para diseñar una propuesta de un marco de trabajo genérico adaptable, que sea capaz de brindar los lineamientos para realizar la implementación de un modelo de madurez, el cual permite medir la seguridad de la información de la organizaciones. A continuación se presenta un resumen de la revisión bibliográfica desarrollada:

A. **"Modelo de Madurez de la Gestión de la Seguridad Informática en el contexto de las Organizaciones Inteligentes".** (Marianella Villegas, 2009).

   Este artículo ofrece una propuesta de un modelo de madurez para la Gestión de la Seguridad de la Información partiendo del punto de vista de las Organizaciones

Inteligentes, las cuales se enmarcan en cinco disciplinas: el dominio personal, los modelos mentales, la visión compartida, el aprendizaje en equipo y el pensamiento sistémico. El modelo está integrado por 5 niveles: Inicio, Crecimiento, Desarrollo, Madurez Organizacional e Inteligencia Organizacional. Con ello se busca disminuir la complejidad y la incertidumbre en la gestión de la seguridad de la Información en las organizaciones lo que contribuirá a la fácil identificación de las herramientas de hardware y software para proteger los activos informáticos. Para desarrollar este artículo los autores realizaron una investigación de tipo exploratorio a través de entrevistas estructuradas a personal experto, asesores de empresa, profesores del área de seguridad, revisión de textos, sitios web entre otros. Los autores han desarrollado diferentes artículos sobre temas relacionados por lo que cuentan con experiencia en el campo. La bibliografía utilizada es diversa y es de destacar que incluyen otros artículos desarrollados por los mismos autores. Esta investigación brinda una idea de los aspectos de la seguridad informática.

B. "DF-C2M2: A Capability Maturity Model for Digital Forensics Organisations". (Ebrahim Hamad Al-Hanaei, 2014).

En este artículo los autores intentan contribuir a la problemática que han descubierto en el área de forense digital, en este campo las evidencias digitales de una investigación deben cumplir requerimientos legales para ser considerada, además los laboratorios forenses digitales deben cumplir requerimientos y ser acreditados con la ISO17025, es por ello que proponen un modelo de capacidad de madurez que permita a las organizaciones evaluar el nivel de madurez de sus capacidades de forense digital. Dicho modelo permite medir la madurez a través de tres dimensiones: personas, procesos y herramientas. Este modelo se ha operasionalizado en una herramienta, y permite definir, evaluar y medir el nivel de madurez de los laboratorios de forense digital, han determinado que la madurez puede estar dentro de 6 niveles, nivel 0: personas dependientes de práctica, nivel 1: Procesos documentados, nivel 2: Despliegue Parcial, nivel 3: Despliegue Completo, nivel 4: Medido y Automatizado y nivel 5: Mejora Continua.

Los datos se obtuvieron a través de una encuesta en línea realizada a expertos en el área de Forense digital en laboratorios privados, agencias federales y entrevistas directas a expertos en este campo. Uno de los autores cuenta con amplia experiencia al ser profesor y director de seguridad de la Universidad de Lancaster. Este artículo es de utilidad ya que nos permite observar la diversidad de aplicaciones que pueden tener los modelos de madurez y la utilidad que brinda su implementación a las organizaciones sobre todo a la Seguridad.

C. "Open Information Security Management Maturity Model (O-ISM3)". (Aceituno, 2011).

Este documento describe el marco de trabajo Open Information Security Management Maturity Model (O-ISM3), el cual ha sido desarrollado por el consorcio Open Group y su objetivo es la administración de la seguridad de la información. En el documento se

describe la forma en que este marco de trabajo se debería desarrollar y cuáles son sus beneficios.

A lo largo del documento se describe como el marco de trabajo O-ISM3 define la madurez en términos de los procesos clave de la seguridad, como define la capacidad en términos de las métricas y la administración de las prácticas utilizadas, para todo ello se describen los principales conceptos utilizados. El documento es una guía clara de cómo se puede implementar este marco de trabajo, los procesos que las Organizaciones deben considerar así como el contexto del negocio, además de describir paso a paso los diferentes tipos de implementación que se pueden desarrollar.

D. "An Approach to Implementing Maturity Models in IT Security". (Rao, 2003).

El artículo se basa en el planteamiento de un nuevo enfoque para implementar modelos de madurez en la seguridad de la información, su investigación se basa en diferentes bibliografías de diversos autores de compañías reconocidas. Dichos autores se mencionan a lo largo del artículo para sustentar los argumentos que van planteando. La propuesta principal de su análisis es un nuevo enfoque basado en tres categorías principales: procesos, aseguramiento y métricas; ellos plantean que las categorías se complementan pero se evalúan de forma individual, además se propone la utilización de un proceso de mejora continua. El modelo de madurez plantea cinco niveles Inicial, Repetible, Definido, Administrado y Optimizado.

Este trabajo presenta dentro de sus argumentos que las mediciones son útiles para establecer una línea base de mejora, el mismo argumento es planteado en el artículo "The Information Security Focus Area Maturity Model" donde los autores mencionan el principio basado en el pensamiento de Lord Kelvin "You cannot improve what you cannot measure" es decir que la seguridad no puede ser mejorada sino puede ser medida. El autor Vasant Rao cuenta con diferentes especialidades entre las cuales se encuentra evaluación con modelos de madurez de seguridad de TI y más de 8 años de experiencia en el área de Seguridad de la Información. Este artículo permite establecer que para que un software sea de calidad su proceso debe ser de calidad por lo que para que un modelo de madurez sea efectivo su proceso de implementación debe ser efectivo.

E. "MGSM-PYME: Metodología para la gestión de la seguridad y su madurez en las PYMES". (Sanchez, Villafranca, Fernandez-Medina, & Piattini, 2009).

El artículo desarrolla una metodología para la gestión de la seguridad y su madurez adaptada para las PYMES. La metodología pretende ser sencilla de aplicar, lo más automatizada posible y que brinde un resultado rápido. Adicionalmente ofrece generar una de las mejores configuraciones más esta no pretende ser la óptima, priorizando en ahorro de costos aunque sacrificando un poco la precisión, pero que al final busca garantizar que los resultados cuenten con una calidad aceptable. En cuanto a la validez de la información presentada en el artículo está basada en buena parte en la sustentación bibliográfica y para demostrar la validez de la metodología los autores han definido un

modelo o esquema base, el cual permite soportar los resultados generados durante la investigación y que de esta manera la metodología cumple los objetivos planteados.

Se establece que la validez de la información del artículo se sustenta en parte en las referencias bibliográficas y según los análisis son sólidos ya que buena parte son basadas en estándares, metodologías, marcos de trabajos, guías de buenas prácticas de reconocimiento internacional y también porque las referencias sustentan de forma integral el tema desarrollado por los autores. Por otro lado la autoridad de los autores uno de los principales, desarrollo su tesis doctoral precisamente en la propuesta planteada, los otros autores cuentan amplia experiencia en las temáticas del artículo. La propuesta principal de análisis de los autores es la definición de una metodología para el desarrollo, implantación y mantenimiento de SGSI y su madurez. Adaptada a necesidades de la organizaciones de las Pymes y sus recursos disponibles, la metodología pretende que sea lo más automatizada posible, de fácil y rápida aplicación y que ahorre costos para esto los autores proponen una herramienta o aplicativo.

Con respecto a la comparación con otras propuestas, esta principalmente se enfoca a la implementación a PYMES mientras que las otras no se limitan a un sector específico, otra diferencia es que esta se orienta tanto a la implementación de un sistema de seguridad de la información y su madurez mientras que las otras propuestas analizadas se enfocan principalmente en el modelo de madurez y por ultimo las otras propuestas definen únicamente la metodología y esta propone adicional una herramienta o aplicativo..

F. **"Program Review for Information Security Management Assistance (PRISMA)".** (Bowen & Kissel, 2007).

Este documento contiene una guía explicativa sobre la metodología (PRISMA) que por sus siglas se define como Program Review for Information Security Management Assistance o Programa de Revisión para la Asistencia de Gestión de la Seguridad de la Información y ha sido desarrollado por el National Institute of Standards and Technology (NIST). Prisma es una herramienta desarrollada e implementada por NIST para la revisión de los complejos requisitos de la información de la seguridad.

Este documento es una explicación del propósito de esta metodología, hacia quienes va dirigido, los diferentes pasos que las organizaciones deben desarrollar para su implementación. En él se describe el programa que utiliza esta metodología, las áreas principales de la información de la seguridad que se pueden evaluar, los diferentes niveles de madurez que se consideran, como puede analizarse la información obtenida y los diferentes reportes que se pueden obtener con la implementación de esta metodología por las Organizaciones.

G. **"Estudio Aplicación del Modelo de Madurez Capacidad de Ingeniería en Seguridad de los Sistemas (SSE-CMM) por áreas de Proyecto y Organización".** (José Antonio Calvo-Manzano, 2003).

El tema central de este artículo es evaluar la madurez de la seguridad de las empresas de los estudiantes de la maestría en auditoría y seguridad informática de la Universidad Politécnica de Madrid basado en el modelo de madurez de seguridad SSE –CMM, utilizando un método de evaluación desarrollado por un grupo de investigación denominado SOMEPRO y constituido por una alianza de tres universidades de España. El estudio principalmente se enfoca en determinar que prácticas del modelo son más utilizadas y que prácticas requieren mayor atención o son poco conocidas por la muestra utilizada durante la investigación.

Con respecto a la validez de los datos se considera que la falta de experiencia y conocimiento de los encuestados pudo haber arrojado datos no tan precisos debido a las limitaciones que se encontraron los investigadores, mencionadas en el artículo. En la investigación los autores se sustentan en diferentes referencias, dentro de las cuales se encuentra el modelo de madurez aplicado en el estudio, las fuentes utilizadas les permiten sustentar el modelo de madurez a aplicar SSE- CMM y una comparación de metodologías de aplicación de dicho modelo, seleccionando al final una de ellas para realizar el estudio.

El estudio propone principalmente en su análisis, evaluar el estado actual de la seguridad tomando como referencia el SSE-CMM, sus objetivos principales son: determinar prácticas que son utilizadas por la mayoría de los participantes que están bien documentadas, determinar que practicas requieren de una mayor atención o son poco conocidas por los participantes y dar conclusiones generales y lecciones aprendidas. Comparando este artículo con otros autores, proponen el uso de una metodología de aplicación del modelo de madurez SSE-CMM evaluado en el estudio, a diferencia de los otros autores analizados que no hacen dicha propuesta. La metodología estudiada en el artículo está diseñada como un estándar para que las organizaciones evalúen la seguridad, el artículo hace referencia a tres modelos de aplicación del SSE-CMM.

H. **"Model-Based IT Governance Maturity Assessments with Cobit".** (Marten Simonsson, 2007).

Los investigadores en este artículo presentan una propuesta de un modelo de evaluación de madurez para la gobernanza de TI diseñado para sobrepasar los problemas de validez, confiabilidad y costos que presentan otros modelos. Ellos plantean el problema de que los objetivos de Control para la Información y Tecnología de COBIT requieren un analista experto para realizar el análisis de madurez al Gobierno de TI además que el marco actual en esta área es vago y ambiguo y llevarlo a la práctica para evaluar la madurez del Gobierno de TI implica altos costos. En este artículo se propone un método para la evaluación de la madurez del Gobierno de TI dentro de una Organización, cumpliendo los requerimientos de validez, confiabilidad y bajo costo.

Los autores proponen un Marco basado en 6 niveles del 0 al 5, donde se evalúan los documentos con los que se cuenta y el monitoreo de los KPI/KGI. La aplicación de dicho marco propuesto fue probada en un pequeño caso de estudio.

Durante el desarrollo del artículo los autores utilizan diversidad de referencias bibliográficas, las cuales son utilizadas para reafirmar sus argumentos. Uno de los autores ha desarrollado diversos artículos en el tema desde 2004 y actualmente es profesor y director del departamento de información industrial y control de sistemas del Instituto Tecnológico Royal en Estocolmo, Suecia. En este artículo se plantea la complejidad que puede tener el aplicar la evaluación de Madurez de COBIT, destacando que es necesario contar con un experto para poder desarrollarlo, COBIT es uno de los modelos que se ha considerado evaluar para el trabajo y este artículo reafirma la complejidad que puede tener la implementación de este modelo de madurez.

I. **"Systems Security Engineering Capability Maturity Model (SSE-CMM)".** (Carnegie Mellon University, 1999).

Este manual es una descripción del modelo SSE-CMM que ha sido desarrollado por el trabajo en conjunto de diferentes individuos y organizaciones con el apoyo de la Universidad Carnegie Mellon. SSE-CMM es un modelo que describe las características esenciales de los procesos de la ingeniería de la seguridad que las organizaciones tienen que tener para asegurar una buena ingeniería de la seguridad, es una métrica estándar para las prácticas de ingeniería de la Seguridad. A lo largo de este documento se describe lo que este modelo considera, la arquitectura en la que está basada, la forma en que este modelo debe implementarse y los requerimientos que se necesitan para desarrollarlo.

J. **"COBIT Process Assessment Model (PAM) using COBIT 4.1".** (ISACA, 2011)

Este documento describe el modelo de evaluación de procesos COBIT PAM que se basa en COBIT 4.1. Sirve como referencia para conocer el propósito de dicho modelo, el alcance y los objetivos para lo cual fue desarrollado, en que se diferencia con el modelo de COBIT 4.1. Además describe cuál es su relación con la ISO/IEC 15504.

COBIT Process Assessment Model (PAM) es un modelo que, tomando como base la norma ISO/IEC 15504, está orientado a la evaluación de procesos de TI dentro de las organizaciones. En este documento se define el conjunto mínimo de requisitos para llevar a cabo una evaluación que asegure que los resultados son consistentes, repetibles y representativos de los procesos evaluados. Además de describir la capacidad del proceso en dos dimensiones, capacidad y proceso.

También en el documento se describen los indicadores de evaluación, que hay dos tipos de indicadores de evaluación:

- Indicadores de capacidad de los procesos, que se aplican a los niveles de capacidad de 1 a 5.

- Los indicadores de desempeño de los procesos, que se aplican exclusivamente al nivel de capacidad 1.

Además de describir los niveles de capacidad utilizados, procesos, atributos de procesos y dominios considerados. En general brinda una descripción completa del modelo.

K. "The Information Security Focus Area Maturity Model". (Marco Spruit, 2014).

El artículo presenta como tema central la propuesta de un modelo de madurez para mejorar la seguridad de la información de una organización a un nivel alto en una forma estructurada, con su investigación pretenden responder la interrogante ¿Cómo puede un modelo de madurez estar diseñado para ayudar a reducir la brecha entre las necesidades de una organización y su nivel actual de seguridad de la información para ayudar a mejorar la madurez de la seguridad de la información de una manera estructurada y eficaz?. Los autores presentan un modelo de madurez para la seguridad de información (ISFAM), en el artículo presentan el enfoque de su investigación para determinar los componentes del modelo de madurez, un ejemplo de cómo pueden ser diseñadas las áreas, la presentación del modelo ISFAM, que tiene 13 áreas de enfoque divididas en cuatro categorías y una implementación del modelo a una empresa.

Para poder tener validez en su propuesta los investigadores desarrollaron entrevistas a personas expertas en el área de Seguridad de la Información pertenecientes a diversas empresas, los autores utilizan diversidad de referencias bibliográficas las cuales utilizan a lo largo del artículo para reafirmar sus argumentos.

Los autores que desarrollaron el artículo tienen conocimientos en el área de Negocios Informáticos, trabajan actualmente en la universidad Utrecht de Holanda y en Deloitte, lo que les brinda experiencia en el tema desarrollado. En este artículo los autores proponen un modelo de madurez para la Seguridad de la Información, tema que da un acercamiento de cómo se aplica un modelo de madurez para apoyar la seguridad de la información a diferentes organizaciones.

L. "Information Security Maturity Model. *International Journal of Computer Science and Security".* (Saleh, 2011).

El artículo se centra en una propuesta de modelo de madurez de la seguridad de la información de amplia gama que intenta ser una herramienta para evaluar habilidades de las organizaciones para alcanzar los objetivos de la seguridad. Con respecto a la validez de los datos no se encontró ningún dato que demuestre que el modelo propuesto sea efectivo, más sin embargo el autor menciona que los resultados del articulo muestran que existen indicadores que permiten evaluar la implementación de la seguridad en la organización, utilizando un método cualitativo para demostrarlo, pero que este no es tan fiable por ser subjetivo. El articulo presenta referencias primarias como la de un modelo de madurez de la seguridad de la información denominado ISM3, existen referencias de

organizaciones internacionales relacionadas a la seguridad, en este sentido se considera que el articulo cuenta con solidez referencial. Se considera al autor experto en seguridad. Para el caso de la propuesta principal es desarrollar una herramienta para evaluar la capacidad de las organizaciones con respecto al cumplimiento de los objetivos de seguridad, la confidencialidad, integridad y disponibilidad, definiendo un modelo de un proceso que gestiona, mide y controla todos los aspectos de seguridad basado en indicadores y orientado a dominios. El artículo presenta una propuesta de evaluación basada en cumplimento en diferentes niveles y aspectos, para el caso de los otros autores los modelos de madurez propuestos no denominan sus niveles de cumplimiento. Finalmente el autor plantea un modelo de madurez para la seguridad de la información y propone como este debe ser orientado para su implementación.

M. *"Principles of Information Security".* (Michael E. Whitman, 2012).

Este libro permite conocer más sobre la Seguridad de la información, en él se puede encontrar la definición de lo que es la seguridad de la información, un poco de su historia como se ha desarrollado este concepto a lo largo de los años, los principales conceptos de seguridad de la información que deben conocerse o considerarse al hablar de este tema.

En este documento se logra conocer la información básica, conceptos, componentes, ciclo de vida, roles que se pueden encontrar en los temas que tratan sobre la Seguridad de la Información.

N. "Presenting a Model for Ranking Organizations Based on the Level of the Information Security Maturity". (Nobari, 2011).

El objetivo de este artículo es establecer un ranking organizacional sobre el nivel de la madurez seguridad de la información mediante la presentación de un modelo basado en el conocimiento de multi-criterios para la toma de decisiones. Se han estudiado los modelos y normas que se presentan en la madurez de seguridad de la información. Después se ha determinado los criterios de seguridad de la información en las técnicas y formas de gestión, se han tomado en cuenta los criterios de la triada de la seguridad como son: la confiabilidad, la integridad y disponibilidad, se les ha asignado peso mediante el uso de puntos de vista de los expertos en los departamentos de TI de las tres organizaciones elegidas para el estudio.

Los autores poseen diferentes especialidades destacándose entre ellas sobre Gestión de Tecnologías de la Información, otro aspecto es como miembro de una Editorial Internacional de la Seguridad de la Información y Gestión de Sistemas. Adicionalmente, han ganado muchos premios como mejor investigador en el ramo de las Ciencias de Gestión.

Esta investigación se ha realizado en tres fases principales como primera parte la verificación de los criterios para la evaluación del nivel de madurez de seguridad de información, en segundo lugar los criterios de ponderación, donde se emplean modelos

matemáticos y en tercer lugar la clasificación de las organizaciones basada en el nivel de la madurez seguridad de la información.

Este artículo posee una fundamentación teórica de ciertos marcos de referencia entre ellos las ISO 27000 y el modelo de madurez de COBIT, además que posee una gama de referencias bibliográficas. Esta investigación trata de unir varios conceptos de toma de decisiones de los criterios de seguridad de la información de evaluación de los problemas de la madurez de un enfoque diferente y el uso de las matemáticas. De hecho, los expertos de seguridad de la información, pueden considerar los criterios en la evaluación de la madurez de seguridad de la información en función de su valor e importancia y mediante la introducción del elemento de ponderación.

O. "Developing Maturity Models for IT Management – A Procedure Model and its Application". (Becker, 2009)**.**

El objetivo de este artículo es proponer un modelo de procedimiento para el diseño de modelos de madurez con la idea de remediar las deficiencias generalizadas, se destaca la importancia de que un modelo de madurez mejora el posicionamiento de la organización y ayuda a encontrar mejores soluciones para el cambio. Considerando que los procedimientos y métodos que llevan muchos modelos sólo se han documentado muy someramente. Este artículo posee un enfoque científico, habiendo desarrollado criterios para el desarrollo de modelos de madurez. Estos criterios también sirven como base para la comparación de los enfoques de madurez escasamente documentados.

Se han tomado como referencia diferentes diseños de procesos de Modelos de Madurez como son ACMM, BPMM, CMMI, DPMM entre otros marcos de trabajo, hay un proceso definido que realiza una comparación entre los modelos, un procedimiento iterativo con literatura investigativa y entrevista de expertos, posteriormente se evalúa los modelos, el uso de procedimientos multi -metodológicos, se identifican la relevancia del problema, se define el problema y la publicación de resultados relevantes.

Se han tomado un estudio de 51 modelos de madurez, hay referencias bibliográficas en diferentes fases del documento, los autores poseen conocimientos sobre diferentes áreas de gestión y enfoques de modelos de madurez, con gran experiencia profesional en el ramo.

Este caso de estudio se ilustra la aplicabilidad de este modelo. Los resultados de este estudio se han creado para servir como manual para los diseños y evaluaciones metódicamente fundados en modelos de madurez. Mediante la aplicación de las directrices que Hevner ha propuesto para el diseño de modelos de madurez, ocho requisitos fueron postulados para el proceso de diseño y un modelo de procedimiento adecuado se ha realizado. Esto proporciona un marco sólido para el desarrollo metodológicamente fundado y evaluaciones de modelos de madurez. El propósito

principal del modelo de procedimiento es crear conciencia para un diseño de modelo de madurez metodológicamente bien fundamentados. Los resultados nos llevan a un modelo de procedimiento genérico y consolidado para el diseño de modelos de madurez.

P. ISO/IEC 21827:2002 Ingeniería de Sistemas de Seguridad - Modelo de Capacidades de Madurez (SSE-CMM) (ISO/IEC, 2002)

El objetivo de este ISO/IEC 21827:2002 es proveer directrices y lineamientos de como utilizando la Ingeniería se puede aplicar a toda la organización en diferentes aspectos, tiene un enfoque especifico de procesos y se puede integrar a las diferentes ramas de la Ingeniería. La Ingeniería de Sistemas de Seguridad - Modelo de Capacidades de Madurez (SSE-CMM) describe las características esenciales del proceso de ingeniería de seguridad de una organización que debe existir para asegurar una buena ingeniería de seguridad. El SSE-CMM no prescribe un proceso o secuencia particular, pero captura prácticas observadas generalmente en la industria.

La Ingeniería de Sistemas de Seguridad - Modelo de Capacidades de Madurez (SSE-CMM) está diseñado para todas las organizaciones .El uso del SSE-CMM no debe implicar que uno de los enfoques es mejor que el otro o que cualquiera de estos usos son obligatorios. El enfoque de negocio de una organización no necesita ser parcializado por el uso de la SEE-CMM.

Basado en el enfoque de la organización, algunas, pero no todas, de las prácticas de ingeniería de seguridad definidos se pueden aplicar. Además, la organización podría tener que visualizar a las relaciones entre las diferentes prácticas dentro del modelo para determinar su aplicabilidad. El SSE-CMM puede ser aplicado a software, sistemas, facilidades de desarrollo y operaciones para una variedad de tipos de organizaciones.

2.3 Bases Teóricas

Después de analizar a través de la revisión bibliográfica una variedad de investigaciones, modelos y/o marcos de trabajo se definieron ciertos criterios de evaluación como: la capacidad de adaptabilidad, es decir, que pueda implementarse cualquier tipo y tamaño de organización, la facilidad de comprensión del equipo implementador, reconocimiento internacional y la opinión de un experto, para seleccionar los siguientes modelos o metodologías como aportes principales del diseño de la propuesta del marco de trabajo genérico que permita medir la madurez de la seguridad de la información de las organizaciones.

2.3.1 ISO/IEC 21827:2002 Ingeniería de Sistemas de Seguridad - Modelo de Capacidades de Madurez (SSE-CMM) (ISO/IEC, 2002)

Introducción

Una amplia variedad de organizaciones practican ingeniería de la seguridad en el desarrollo de programas de computación, ya sea como software de sistemas operativos, gestión

de seguridad y funciones de aplicación, software, middleware de programas de aplicaciones, entre otros.

Por lo tanto, los métodos y las prácticas adecuadas son requeridos por los desarrolladores de productos, proveedores de servicios, integradores de sistemas, administradores de sistemas, e incluso los especialistas en seguridad. Algunas de estas organizaciones se ocupan de cuestiones de alto nivel (por ejemplo, los relacionados con el uso operativo o la arquitectura del sistema), otros se centran en cuestiones de bajo nivel (por ejemplo, mecanismo de selección o diseño)y algunos lo hacen ambos. Las organizaciones pueden especializarse en un tipo particular de tecnología, o un contexto especializado.

La Ingeniería de Sistemas de Seguridad - Modelo de Capacidades de Madurez (SSE-CMM) está diseñado para todas las organizaciones. El uso del SSE-CMM no debe implicar que uno de los enfoques es mejor que el otro o que cualquiera de estos usos son obligatorios. El enfoque de negocio de una organización no necesita ser parcializado por el uso de la SEE-CMM.

Basado en el enfoque de la organización, algunas, pero no todas, las prácticas de ingeniería de seguridad definidos se pueden aplicar. Además, la organización podría tener que visualizar a las relaciones entre las diferentes prácticas dentro del modelo para determinar su aplicabilidad. El SSE-CMM puede ser aplicado a software, sistemas, facilidades de desarrollo y operaciones para una variedad de tipos de organizaciones.

A continuación se presenta algunas tipos de organizaciones:

Proveedores de Servicios de Seguridad

Para medir la capacidad de los procesos de una organización que lleva a cabo las evaluaciones de riesgos, varios grupos de prácticas entran en juego. Durante el desarrollo del sistema o integración, habría que evaluar la organización con respecto a su capacidad para determinar y analizar las vulnerabilidades de seguridad y evaluar los impactos operacionales. En el caso de funcionamiento, habría que evaluar la organización con respecto a su capacidad para vigilar la situación de seguridad del sistema, identificar y analizar las vulnerabilidades de seguridad y evaluar los impactos operacionales.

Desarrolladores de Contramedidas

En el caso de un grupo que se centra en el desarrollo de las contramedidas, la capacidad de proceso de una organización se caracteriza por una combinación de prácticas SSE-CMM®. El modelo contiene prácticas para hacer frente a la determinación y el análisis de las vulnerabilidades de seguridad, la evaluación de los impactos operativos, proporcionar información y orientación a otros grupos involucrados (como un grupo de software). El grupo que ofrece el servicio de contramedidas en desarrollo necesita entender las relaciones entre estas prácticas.

Desarrolladores de producto

El SSE-CMM incluye prácticas que se centran en profundizar en el conocimiento de las necesidades de seguridad del cliente. Se requiere la interacción con el cliente para verificar estos. En el caso de un producto, el cliente es genérico como el producto desarrollándose independientemente priori de un cliente específico. Cuando este es el caso, el grupo de marketing de producto u otro grupo se pueden utilizar como el cliente hipotético, si se requiere.

Los profesionales en ingeniería de seguridad reconocen que los contextos de productos y los métodos utilizados para llevar a cabo el desarrollo de productos son tan variados como los propios productos. Sin embargo, hay algunas cuestiones relacionadas con el contexto de producto y proyecto que se sabe que tienen un impacto en la forma en que los productos son concebidos, producidos, entregados, y mantenidos. Los siguientes temas, en particular, tienen importancia para el SSE-CMM:

- Tipo de base de clientes (productos, sistemas o servicios);
- Aseguramiento de requisitos (alto versus bajo);
- Apoyo para el desarrollo y organizaciones operacionales.

A continuación se analizan las diferencias entre dos diversas bases de clientes, diferentes grados de requisitos de garantía, y el impacto de cada una de estas diferencias en la SSE-CMM. Estos se proporcionan como un ejemplo de cómo una organización o segmento de la industria podrían determinar el uso apropiado de la SSE-CMM en su entorno.

Específico Segmento de la Industria

Cada industria refleja su propia cultura, la terminología y el estilo de comunicación en particular. Al minimizar las dependencias de roles e implicaciones de la estructura de la organización, se provee que los conceptos SSE-CMM pueden ser fácilmente traducidos por todos los segmentos de la industria en su propia lengua y cultura.

Forma de cómo debería ser usado el SSE-CMM

El SSE-CMM y el método para la aplicación del modelo (es decir, el método de valoración) están destinados a ser utilizados como:

- Herramienta para organizaciones de ingeniería para evaluar sus prácticas de ingeniería de seguridad y definir las mejoras.
- Método de las organizaciones de evaluación de la ingeniería de seguridad tales como certificadores y evaluadores pueden establecer la confianza en la capacidad de la organización como una entrada al sistema o la garantía de la seguridad de los productos.
- Mecanismo estándar para los clientes para evaluar la capacidad de ingeniería de seguridad de un proveedor.

Las técnicas de evaluación pueden ser utilizados en la aplicación del modelo para la auto mejora y en la selección de proveedores, si los usuarios de los modelos y los métodos de evaluación del modelo hacen entender a fondo la correcta aplicación del modelo y sus limitaciones inherentes.

Ventajas de utilizar el SEE-CMM

La tendencia de la seguridad es un cambio de la protección de datos clasificados del gobierno a un espectro más amplio de preocupaciones incluyendo las transacciones financieras, acuerdos contractuales, información personal y el Internet. Ha surgido una proliferación correspondiente de productos, sistemas y servicios que mantienen y protegen la información. Estos productos y sistemas de seguridad normalmente llegan al mercado de dos maneras: a través de una larga y costosa evaluación o sin evaluación. En el primer caso, los productos de confianza a menudo llegan al mercado mucho después de que sus características son necesitadas y sistemas de seguridad están siendo desplegados donde ya no dan respuesta a las amenazas actuales. En

este último, los compradores y los usuarios deben depender únicamente de las exigencias de seguridad de los desarrolladores de sistema, producto o el operador. Además, los servicios de ingeniería de seguridad tradicionalmente se comercializan frecuentemente sobre esta base.

Esta situación requiere de organizaciones para practicar la ingeniería de seguridad de una manera más madura. En concreto, se necesitan las siguientes cualidades en la producción y el funcionamiento de los sistemas seguros y productos confiables:

- **Continuidad** - conocimientos adquiridos en los esfuerzos anteriores se utiliza en los futuros esfuerzos.
- **Repetitividad** - una forma de garantizar que los proyectos puedan repetir un exitoso esfuerzo.
- **Eficiencia** - una manera de ayudar a los desarrolladores y evaluadores a trabajar de manera más eficiente.
- **Aseguramiento** - confianza en que las necesidades de seguridad están siendo abordadas.

Para proporcionar estos requisitos, se necesita un mecanismo para guiar a las organizaciones a comprender y mejorar sus prácticas de ingeniería de seguridad. Para hacer frente a estas necesidades, la SSE-CMM se está desarrollando para avanzar en el estado de la práctica de la ingeniería de seguridad con el objetivo de mejorar la calidad, la disponibilidad, reducir el costo de la entrega de sistemas seguros, productos de confianza y servicios de ingeniería de seguridad.

Alcance

El SSE-CMM es un modelo de referencia de proceso. Se centra en los requisitos para la implementación de la seguridad en un sistema o conjunto de sistemas relacionados que son del dominio ITS[1]. Dentro del ITS de dominio del modelo SSE-CMM se centra en los procesos utilizados para lograr sus ITS, más específicamente en la madurez de los procesos. No hay ninguna intención en el Modelo SSE-CMM de dictar un proceso específico para ser utilizado por una organización y mucho menos una metodología específica. Más bien la intención es que la organización haciendo uso del Modelo SSE-CMM debería utilizar sus procesos existentes, ya sea aquellos procesos basados en cualquier otro documento de orientación ITS. El alcance abarca:

- Las actividades de ingeniería de la seguridad del sistema para un producto seguro o un sistema de confianza direccionado al ciclo de vida completo: definición del concepto, análisis de requerimientos, diseño, desarrollo, integración, instalación, operación y mantenimiento final de puesta en marcha.
- Requisitos para los desarrolladores de producto, desarrolladores e integradores de sistemas de seguridad, las organizaciones que prestan servicios de seguridad informática y la ingeniería de seguridad informática.
- se aplica a todos los tipos y tamaños de organizaciones de ingeniería de seguridad desde comercial para el gobierno y la academia.

Mientras que el SSE-CMM es un modelo distinto para mejorar y evaluar la capacidad de ingeniería de seguridad, ello no implica que la ingeniería de seguridad deba ser practicada en forma aislada de otras disciplinas de ingeniería. Por el contrario, la SSE-CMM promueve esa

[1] Information Technology Security

integración, al considerar que la seguridad es un fenómeno generalizado en todas las disciplinas de ingeniería (por ejemplo, sistemas, software y hardware) y los componentes que definen el modelo para hacer frente a esas preocupaciones.

Antecedentes.

El Modelo de Capacidad de Madurez de Ingeniería de Seguridad de Sistemas (SSE-CMM) describe las características esenciales del proceso de ingeniería de seguridad de una organización que debe existir para asegurar una buena ingeniería de seguridad. El SSE-CMM no prescribe un proceso o secuencia particular, pero captura prácticas observadas generalmente en la industria. El modelo es una medida estándar para las prácticas de ingeniería de seguridad que cubren:

- El ciclo de vida completo, incluyendo el desarrollo, operación, mantenimiento y actividades de clausura.
- Toda la organización, incluidos las de gestión, las actividades de la organización, y de ingeniería.
- Interacciones concurrentes con otras disciplinas, como el sistema, software, hardware, factores humanos y la ingeniería de prueba; la gestión del sistema, operación y mantenimiento.
- Interacciones con otras organizaciones, incluyendo la adquisición, la gestión del sistema, certificación, acreditación y evaluación.

SSE-CMM está basado en una visión global del modelo, en sugerencias para el uso adecuado del modelo, las prácticas incluidas en el modelo, y una descripción de los atributos del modelo. También incluye los requisitos utilizados para desarrollar el modelo.

Razón para el Desarrollo

Tanto los clientes como los proveedores están interesados en mejorar el desarrollo de productos de seguridad, sistemas y servicios. El campo de la ingeniería de seguridad tiene varios principios generalmente aceptados, pero actualmente carece de un marco global para evaluar las prácticas de ingeniería de seguridad. El SSE-CMM, mediante la identificación de dicho marco, proporciona una manera de medir y mejorar el rendimiento en la aplicación de los principios de la ingeniería de seguridad.

Hay que subrayar que la ingeniería de seguridad es una disciplina única, lo que requiere un conocimiento único, habilidades y procesos que amerita la elaboración de un CMM distinto para la ingeniería de seguridad. Esto no entra en conflicto con la premisa de que la ingeniería de seguridad se lleva a cabo en el contexto de la ingeniería de sistemas. De hecho, después de haber definido y aceptado las actividades de ingeniería de sistemas permitirán prácticas de ingeniería de seguridad de manera efectiva en todos los contextos.

Un moderno control estadístico del proceso sugiere que los productos de más alta calidad se pueden producir de manera más económica, haciendo hincapié en la calidad de los procesos que los producen y la madurez de las prácticas organizacionales inherentes a esos procesos. Procesos más eficientes están garantizados, dado el aumento de los costos y el tiempo requerido para el desarrollo de sistemas seguros y productos de confianza. La operación y mantenimiento de sistemas de seguridad se basa en los procesos que vinculan a las personas y las tecnologías. Estas interdependencias pueden ser manejadas de manera más rentable, haciendo hincapié en la

calidad de los procesos que se utiliza, y la madurez de las prácticas de la organización inherente a los procesos.

El objetivo del Proyecto SSE-CMM es avanzar en la ingeniería de la seguridad como está definido, en la madurez y la disciplina medible. Los modelos y métodos de evaluación SSE-CMM se están desarrollando para permitir que:

- Las inversiones se centren en las herramientas de ingeniería de seguridad, formación, definición de procesos, prácticas de gestión y mejoras por parte de grupos de ingeniería.
- Aseguramiento basada en capacidad, es decir, la confianza basada en la confianza en la madurez de las prácticas y procesos de seguridad de un equipo de ingeniería.
- Selección de proveedores debidamente cualificado de ingeniería de la seguridad a través de la diferenciación de los licitadores por los niveles de capacidad y los riesgos programáticos asociados.

La importancia de la Ingeniería de Seguridad

Con la creciente dependencia de la sociedad de la información, la protección de la información es cada vez más importante; muchos productos, sistemas y servicios son necesarios para mantener y proteger la información. El enfoque de la ingeniería de la seguridad se ha ampliado principalmente concerniente con la salvaguarda o contramedidas clasificando los datos del gobierno para aplicaciones más amplias, incluyendo las transacciones financieras, acuerdos contractuales, información personal y el Internet. Estas tendencias han elevado la importancia de la ingeniería de seguridad.

Arquitectura del Modelo

El SSE-CMM es una recopilación de las prácticas de ingeniería de seguridad más conocidos. Para entender este modelo, se requiere algo de experiencia en ingeniería de seguridad. Esta sección proporciona una descripción de alto nivel de ingeniería de seguridad, a continuación se describe cómo la arquitectura del modelo refleja esta comprensión básica.

Ingeniería de Seguridad

El impulso hacia la interconectividad dominante, interoperabilidad de redes, equipos, aplicaciones, e incluso las empresas está creando un papel más crucial para la seguridad en todos los sistemas y productos. El enfoque de la seguridad ha pasado de salvaguardar los datos clasificados del gobierno, para una aplicación más amplia, incluyendo las transacciones financieras, acuerdos contractuales, información personal y el Internet. Como resultado, es necesario que las necesidades de seguridad potenciales se consideren y se determinen para cualquier aplicación. Los ejemplos de las necesidades a tener en cuenta son: la confidencialidad, la integridad, la disponibilidad, la rendición de cuentas, la privacidad y la seguridad.

El cambio de enfoque de los problemas de seguridad eleva la importancia de la ingeniería de seguridad. Ingeniería de seguridad se está convirtiendo en una disciplina cada vez más crítica, debe ser un componente clave en la multidisciplina y equipos de ingeniería concurrente.

Esto se aplica al desarrollo, integración, operación, administración, mantenimiento y evolución de los sistemas y aplicaciones, así como para el desarrollo, la entrega y la evolución de los

productos. Los problemas de seguridad deben ser abordados en la definición, gestión, reingeniería de las empresas y los procesos de negocio. Ingeniería de seguridad puede entonces ser entregado en un sistema, en un producto o como un servicio.

Descripción de Ingeniería de Seguridad

Ingeniería de seguridad es una disciplina en evolución. Como tal, una definición precisa con el consenso de la comunidad no existe hoy en día. Sin embargo, algunas generalizaciones son posibles. Algunos de los objetivos de la ingeniería de seguridad son:

- Aumentar la comprensión de los riesgos de seguridad asociados con una empresa.
- Establecer un conjunto equilibrado de las necesidades de seguridad de acuerdo con los riesgos identificados.
- Transformar las necesidades de seguridad en una guía de seguridad para ser integrado en las actividades de otras disciplinas que trabajan en un proyecto y en las descripciones de la configuración del sistema o la operación.
- Establecer la confianza o seguridad en la corrección y eficacia de los mecanismos de seguridad.
- Determinar los impactos operacionales que debido a las vulnerabilidades de seguridad residuales en un sistema o su funcionamiento son (riesgos aceptables) tolerables.
- Integrar los esfuerzos de todas las disciplinas de la ingeniería y especialidades en una comprensión conjunta de la fiabilidad de un sistema.

Ciclo de Vida de Ingeniería de Seguridad.

Actividades de Ingeniería de Seguridad son practicadas durante todas las fases del ciclo de vida, incluyendo las etapas de:

- Conceptualización
- Desarrollo
- Producción
- Utilización
- Soporte
- Retirada

Ingeniería de Seguridad y otras disciplinas.

- Ingeniería de la Empresa
- Ingeniería de Sistemas
- Ingeniería de Software
- Ingeniería de Factores Humanos
- Ingeniería de Comunicaciones
- Ingeniería de Hardware
- Ingeniería de prueba
- Administración del sistema

Actividades de ingeniería de seguridad deben coordinarse con muchas entidades externas para el aseguramiento y la aceptabilidad de los impactos operacionales residuales sean establecidos en conjunto con el desarrollador, integrador, adquirente, usuario, evaluador independiente y otros grupos. Son estas interfaces y la interacción necesaria en un amplio

conjunto de organizaciones que conforman la ingeniería de seguridad particularmente complejo y diferente de otras disciplinas de la ingeniería.

Especialistas de Ingeniería de Seguridad.

Mientras la Ingeniería de Seguridad y Tecnología de la Información de Seguridad son muy a menudo las disciplinas de conducción en el entorno de seguridad y de negocio actual, otras disciplinas de seguridad más tradicionales, como la seguridad física y seguridad personal no deben ser pasadas por alto. Ingeniería de Seguridad tendrá que recurrir a estas y muchas otras sub disciplinas especializadas para que puedan lograr los resultados más eficientes y eficaces en el desempeño de su trabajo. La siguiente lista da algunos ejemplos de sub-disciplinas susceptibles de ser necesario, junto con una breve descripción de cada especialidad de seguridad. Ejemplos de la especialidad de
sub disciplinas de seguridad incluyen:

- Operaciones de Seguridad se dirige a la seguridad del ambiente de operación y el mantenimiento de una postura operativa segura.
- Seguridad de la información se refiere a la información y el mantenimiento de la seguridad de la información durante su manipulación y procesamiento.
- Seguridad de la red consiste en la protección de hardware de redes, software y protocolos, incluyendo la información a través de redes.
- Seguridad Física se centra en la protección de los edificios y las ubicaciones físicas.
- Seguridad del personal se relaciona con la gente, su fiabilidad y su conocimiento de los problemas de seguridad.
- Administración de la Seguridad tiene que ver con los aspectos administrativos de la seguridad y la seguridad en los sistemas administrativos.
- Seguridad en las Comunicaciones se relaciona con la comunicación de información entre dominios de seguridad, específicamente la protección de la información mientras se mueve a través del medio de transporte.

Resumen del Proceso de Ingeniería de Seguridad

El SSE-CMM divide ingeniería de seguridad en tres áreas básicas: riesgo, la ingeniería, y el aseguramiento, véase la figura 2. Mientras que estas áreas no son independiente una de la otra, es posible considerarse por separado. Al nivel más simple, el proceso de riesgos identifica y prioriza los peligros inherentes al producto o sistema desarrollado. El proceso de ingeniería de seguridad funciona con las otras disciplinas de ingeniería para determinar y aplicar soluciones a los problemas planteados por los peligros. Finalmente, el proceso de aseguramiento establece la confianza en las soluciones de seguridad y transmite esta confianza a los clientes.

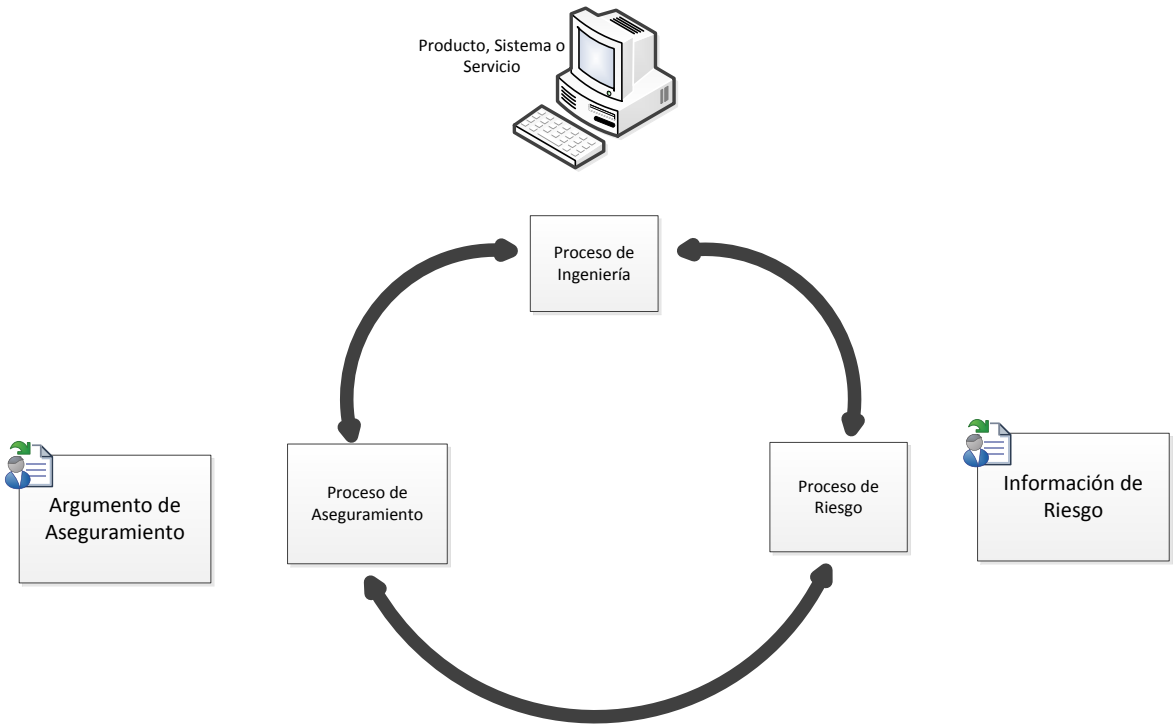


Figura 2. El proceso de Ingeniería de Seguridad con tres principales áreas.

En conjunto, estas tres áreas trabajan juntos con el objetivo de garantizar que el proceso de ingeniería de la seguridad logren los objetivos descritos anteriormente.

Riesgo

Un objetivo importante de la ingeniería de la seguridad es la reducción del riesgo. La evaluación de riesgos es el proceso de identificación de los problemas que todavía no han ocurrido. Los riesgos se evalúan mediante el examen de la probabilidad de la amenaza y la vulnerabilidad y considerando el impacto potencial de un incidente no deseado, ver figura 3. Asociado con esa probabilidad es un factor de incertidumbre, que variará dependiendo de una situación particular. Esto significa que la probabilidad sólo se puede predecir dentro de ciertos límites. Además, el impacto evaluado para un riesgo en particular también está asociado a la incertidumbre, ya que el incidente no deseado puede no resultar como se esperaba. Debido a que los factores pueden tener una gran cantidad de incertidumbre en cuanto a la exactitud de las predicciones asociadas a ellos, la planificación y la justificación de la seguridad puede ser muy difícil. Una forma de abordar parcialmente con este problema de una manera costo-efectiva es la implementación de técnicas para detectar la ocurrencia de un incidente no deseado.

Un incidente no deseado se compone de tres componentes: amenaza, vulnerabilidad e impacto. Las vulnerabilidades son propiedad de los activos que pueden ser explotadas por una amenaza, e incluyen debilidades. Si bien la amenaza o la vulnerabilidad no están presentes, no puede haber ningún incidente no deseado y por lo tanto no hay riesgo. La gestión de riesgos es el proceso de evaluar y cuantificar los riesgos y el establecimiento de un nivel aceptable de riesgo para la organización. La gestión de riesgos es una parte importante de la gestión de la seguridad.

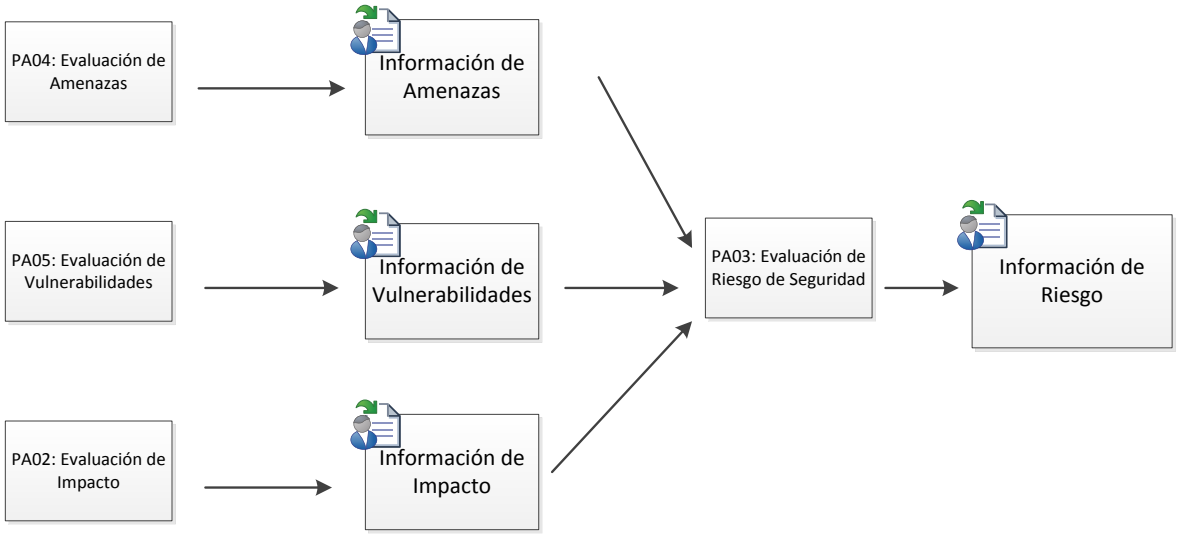


Figura 3. Proceso de Riesgo de la Seguridad envuelve amenazas, vulnerabilidades e impacto.

Los riesgos se ven mitigados por la aplicación de las salvaguardas, lo que puede hacer frente a la amenaza, la vulnerabilidad, el impacto, o el propio riesgo. Sin embargo, no es viable mitigar todos los riesgos o mitigar por completo todo un riesgo particular. Esto es en gran parte debido al costo de la mitigación de riesgos y las incertidumbres asociadas. Por lo tanto, un riesgo residual siempre debe ser aceptado. En presencia de una alta incertidumbre, la aceptación del riesgo se vuelve muy problemático debido a su naturaleza exacta. Una de las pocas áreas bajo el control del tomador de riesgo es la incertidumbre asociada con el sistema. Las áreas de proceso SSE-CMM incluyen actividades que aseguren que la organización de proveedores es el análisis de amenazas, vulnerabilidades, impactos y riesgos asociados.

Ingeniería

Ingeniería de seguridad, al igual que otras disciplinas de la ingeniería, es un proceso que avanza a través de concepto, diseño, implementación, prueba, implementación, operación, mantenimiento y cierre definitivo. A lo largo de este proceso, los ingenieros de seguridad deben trabajar en estrecha colaboración con las otras partes del equipo de ingeniería de sistemas. El SSE-CMM hace hincapié en que los ingenieros de seguridad son parte de un equipo más grande y la necesidad de coordinar sus actividades con los ingenieros de otras disciplinas.

Esto ayuda a asegurar que la seguridad es una parte integral del proceso más grande y no una actividad separada y distinta. Uso de la información del proceso de riesgo descrito anteriormente y otra información sobre los requisitos del sistema, las leyes y políticas; los ingenieros de seguridad trabajan con el cliente para identificar las necesidades de seguridad, ver figura 4. Una vez que se identifican las necesidades, los ingenieros de seguridad identifican y realizan un seguimiento de los requisitos específicos.

El proceso de creación de soluciones a los problemas de seguridad en general implica la identificación de posibles alternativas y luego de evaluar las alternativas para determinar cuál es la más prometedora. La dificultad en la integración de esta actividad con el resto del proceso de ingeniería es que las soluciones no se pueden seleccionar en consideraciones de seguridad

solamente. Más bien, una amplia variedad de otras consideraciones, incluyen el costo, rendimiento, riesgo técnico y facilidad de uso.

Por lo general, estas decisiones deben ser capturadas para reducir al mínimo la necesidad de revisar los temas. Los análisis producidos también constituyen una base importante para los esfuerzos de aseguramiento.

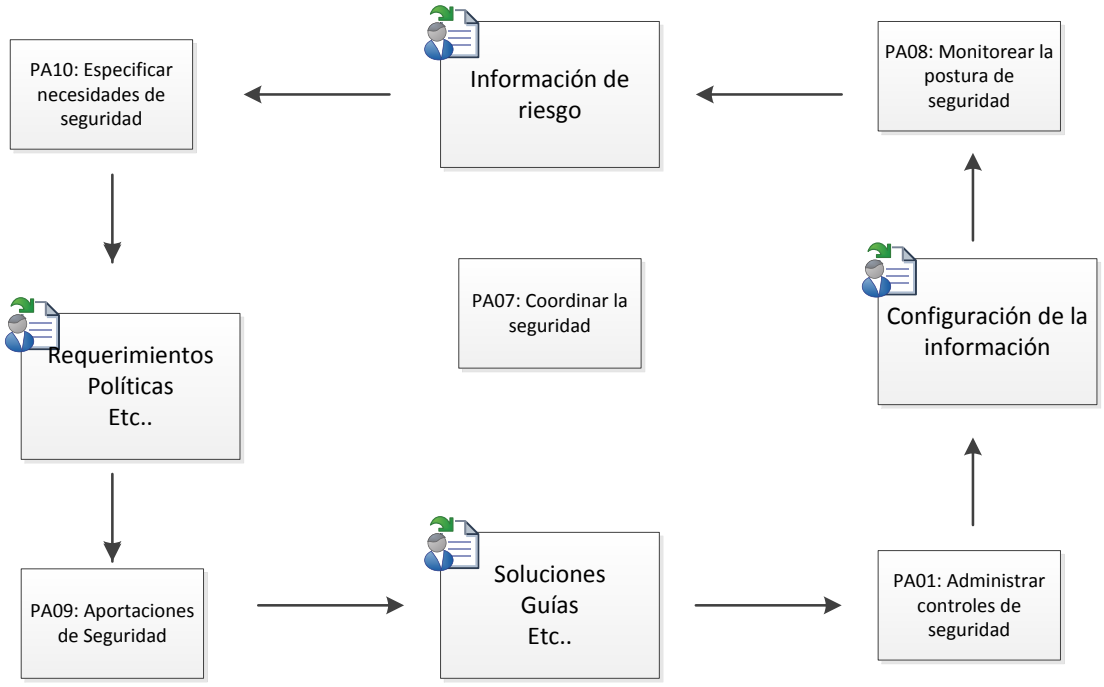


Figura 4. La Seguridad es una parte integral de todos los procesos de Ingeniería.

Más tarde en el ciclo de vida, el ingeniero de seguridad está llamado a garantizar que los productos y los sistemas estén configurados correctamente en relación con los riesgos percibidos, lo que garantiza que los nuevos riesgos no hacen el sistema inseguro para operar.

Aseguramiento

Aseguramiento se define como el grado de confianza en que las necesidades de seguridad se satisfacen [NIST94a]. Se trata de un producto muy importante de la ingeniería de seguridad. Hay muchas formas de aseguramiento. El SSE-CMM® contribuye a un aspecto, la confianza en la repetitividad de los resultados del proceso de ingeniería de seguridad.

La base para esta confianza es que una organización madura es más probable que se repita los resultados que una organización inmadura, véase la figura 5. La relación detallada entre las diferentes formas de aseguramiento es el sujeto de la investigación en curso.

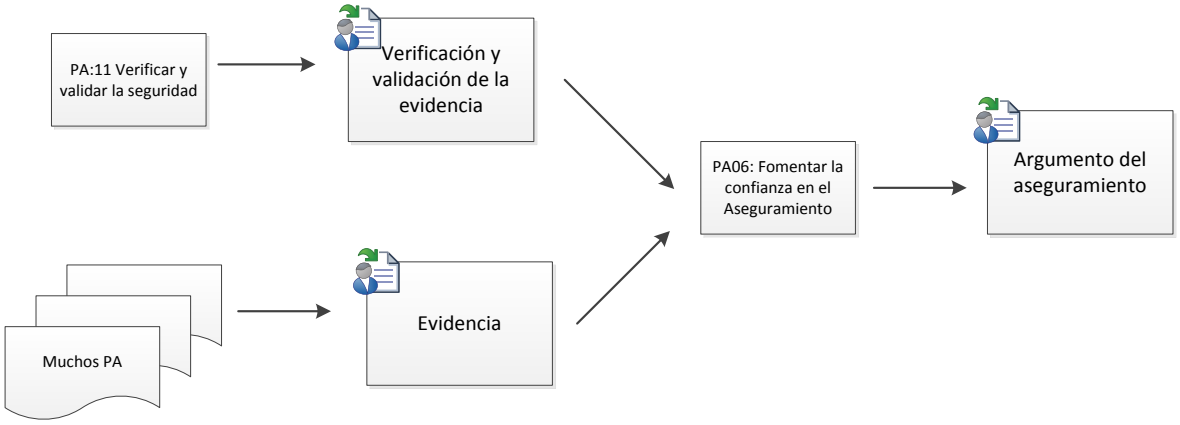


Figura 5. El Proceso de Aseguramiento construye un argumento estableciendo confidencialidad.

Aseguramiento no añade ningún tipo de controles adicionales para contrarrestar los riesgos relacionados con la seguridad, pero proporciona la confianza que los controles que se han implementado reducirán el riesgo previsto.

Aseguramiento también puede ser visto como la confianza de que las salvaguardas funcionarán según lo previsto. Esta confianza se deriva de las propiedades de corrección y eficacia. La corrección es la propiedad que las salvaguardas, como fue diseñado, implementa los requisitos. La eficacia es la propiedad de que las salvaguardas proporcionan seguridad adecuada para satisfacer las necesidades de seguridad del cliente. La fuerza del mecanismo también desempeña un papel, pero es moderado por el nivel de protección y la garantía que se busca.

Aseguramiento a menudo se comunica en forma de un argumento. El argumento incluye un conjunto de afirmaciones sobre propiedades del sistema. Estas afirmaciones están respaldadas por pruebas. La evidencia es con frecuencia en forma de documentación desarrollada durante el curso normal de las actividades de ingeniería de seguridad.

Las actividades SSE-CMM propias implican la producción de aseguramiento de las pruebas pertinentes. Por ejemplo, documentación de procesos puede indicar que el desarrollo ha seguido un proceso de ingeniería bien definido y maduro, que está sujeta a la mejora continua. Verificación de seguridad y validación juegan un papel importante en el establecimiento de la fiabilidad de un producto o sistema. Muchos de los productos ejemplo de trabajo comprendidos dentro de las áreas de proceso contribuirá a formar parte de esa evidencia.

El control moderno estadístico del proceso sugiere que el aumento de la calidad y los productos de seguridad más altos se puedan producir de manera más rentable y en repetidas ocasiones, centrándose en el proceso utilizado para producirlos. La madurez de las prácticas de la organización va a influir y contribuir al proceso.

Descripción de la arquitectura SSE-CMM

La arquitectura SSE-CMM está diseñada para permitir una determinación de la madurez de los procesos de una organización de ingeniería de seguridad en toda la amplitud de la ingeniería de seguridad. El objetivo de la arquitectura es la de separar claramente las características básicas del proceso de ingeniería de la seguridad de sus características de gestión e institucionalización. A fin de garantizar esta separación, el modelo tiene dos dimensiones, llamado "dominio" y "capacidad", que se describen a continuación.

Es importante destacar que el SSE-CMM no implica que ningún grupo o función particular dentro de una organización deban hacer cualquiera de los procesos descritos en el modelo. Tampoco exige que se utilicen mejor y más técnicas o metodología de ingeniería de seguridad. El modelo requiere, sin embargo, que una organización tiene un proceso en el lugar que incluye las prácticas básicas de seguridad descritas en el modelo. La organización es libre de crear su propio proceso y la estructura organizativa de cualquier manera que cumpla con sus objetivos de negocio.

El Modelo Básico

El SSE-CMM tiene dos dimensiones, "dominio" y "capacidad". La dimensión de dominio es quizás la más fácil de las dos dimensiones de entender. Esta dimensión consiste simplemente en todas las prácticas que definen colectivamente la ingeniería de seguridad. Estas prácticas se denominan "prácticas de base." La estructura y el contenido de estas prácticas de base se discuten a continuación.

La dimensión de la capacidad representa las prácticas que indican la gestión de procesos y la capacidad de la institucionalización. Estas prácticas se denominan "prácticas genéricas" que se aplican a través de una amplia gama de dominios. Las prácticas genéricas representan las actividades que se deben realizar como parte de hacer unas prácticas de base.

La Figura 6 ilustra la relación entre las prácticas de base y prácticas genéricas. Una parte fundamental de la ingeniería de la seguridad es la identificación de las vulnerabilidades de seguridad. Una forma de determinar la capacidad de una organización para hacer algo es comprobar si tienen un proceso de asignación de recursos a las actividades que dicen estar haciendo.

Poner la práctica de base y la práctica genérica juntos proporciona una manera de comprobar la capacidad de una organización para llevar a cabo una actividad en particular. Aquí una parte interesada podría preguntar, "¿su organización asigna recursos para la identificación de las vulnerabilidades de seguridad del sistema?" Si la respuesta es "sí", el entrevistador aprende un poco sobre la capacidad de la organización. Responder a todas las preguntas planteadas por la combinación de todas las prácticas de base con todas las prácticas genéricas proporcionará una buena imagen de la capacidad de ingeniería de seguridad de la organización en cuestión.

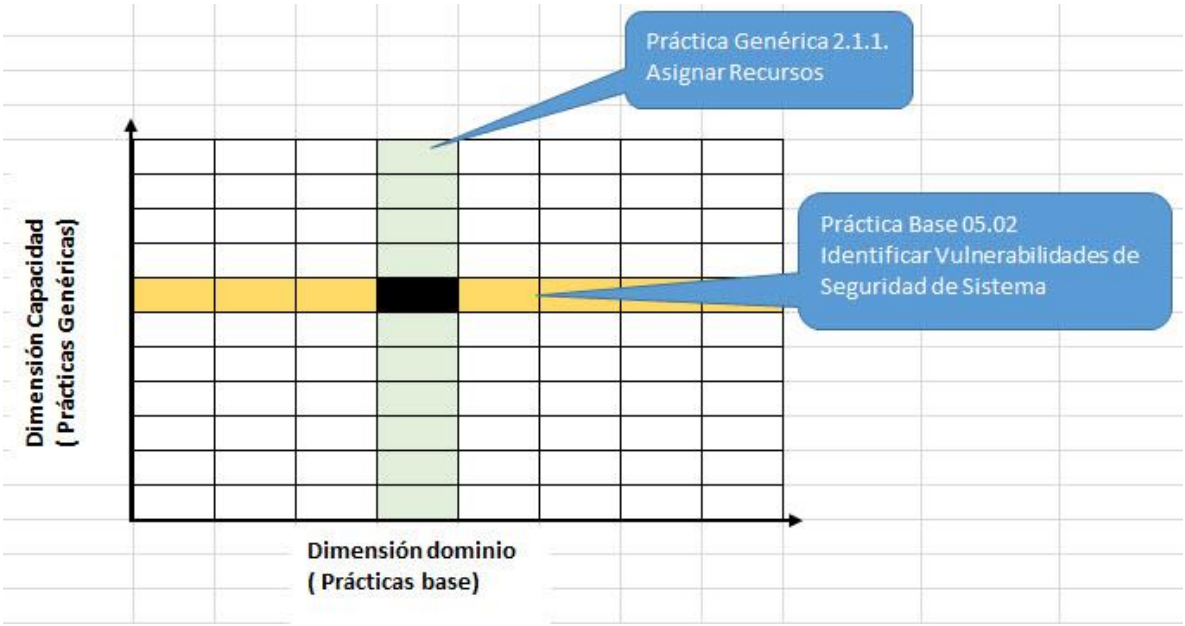


Figura 6. El Proceso de Aseguramiento construye un argumento estableciendo confidencialidad.

Las Prácticas Base

El SSE-CMM contiene 129 prácticas de base, organizados en 22 áreas de proceso. De 61 prácticas base, están organizados en 11 áreas de proceso siendo estas las principales áreas de la ingeniería de seguridad. Las 68 prácticas de bases restantes, organizados en 11 áreas de proceso, direccionados a los dominios de proyecto y organización. Ellos han sido extraídos de la Ingeniería de Sistemas y Software CMM®. Ellas son requeridas a proporcionar un contexto y el apoyo a las áreas de proceso de Ingeniería de Sistemas de Seguridad. Las prácticas básicas de seguridad fueron obtenidas de una amplia gama de materiales existentes, la práctica y la experiencia. Las prácticas seleccionadas representan la mejores prácticas existentes de la comunidad de ingeniería de seguridad, no prácticas no probadas.

La identificación de las prácticas básicas de ingeniería de seguridad se complica por los muchos nombres diferentes para las actividades que son esencialmente los mismos. Algunas de estas actividades ocurren más tarde en el ciclo de vida, en un nivel diferente de abstracción, o normalmente son realizadas por individuos en diferentes roles. Sin embargo, una organización no puede considerarse que haya alcanzado una práctica base si sólo se realiza durante la fase de diseño o en un solo nivel de abstracción. Por lo tanto, la SSE-CMM ignora estas distinciones e identifica el conjunto básico de prácticas que son esenciales para la práctica de la buena ingeniería de seguridad.

Una práctica de base:

- Se aplica en todo el ciclo de vida de la empresa.
- No se superponen con otras Prácticas Comunes.
- Representa una "mejor práctica" de la comunidad de la seguridad.
- No simplemente refleja el estado del arte de la técnica.

- Es aplicable el uso de múltiples métodos en múltiples contextos de negocios.
- No especifica un método o herramienta en particular.

Las prácticas de base se han organizado en las áreas de proceso de una manera que cumpla con un amplio espectro de organizaciones de ingeniería de seguridad. Hay muchas maneras de dividir el dominio ingeniería de la seguridad en las áreas de proceso. Se podría tratar de modelar el mundo real, la creación de áreas de proceso que responden a los servicios de ingeniería de seguridad. Otras estrategias intentan identificar áreas conceptuales que forman los bloques de construcción fundamentales de ingeniería de seguridad. El SSE-CMM compromete entre estas metas competitivas en el actual conjunto de áreas de proceso.

Cada área de proceso tiene un conjunto de metas que representan el estado esperado de una organización que está desempeñando con éxito el área de proceso. Una organización que lleva a cabo las prácticas de base del área de proceso también deberá alcanzar sus metas.

Un área de proceso:

- Ensambla actividades conexas en una zona de fácil uso.
- Se relaciona con valiosos servicios de ingeniería de seguridad.
- Se aplica en todo el ciclo de vida de la empresa.
- se puede implementar en múltiples contextos de organización y de productos.
- Puede ser mejorado como un proceso distinto.
- Puede ser mejorado por un grupo con intereses similares en el proceso.
- Incluye todas las prácticas básicas que se requieren para cumplir con los objetivos del área de proceso.

Las áreas de proceso de ingeniería de seguridad de sistemas son once en la SSE-CMM se enumeran a continuación. Tenga en cuenta que se enumeran en orden alfabético para desalentar la idea de que las áreas de proceso están clasificadas por la fase del ciclo de vida o área. Se enumeran a continuación:

- PA01 Administrar controles de la seguridad
- PA02 Evaluar el impacto
- PA03 Evaluar riesgos de seguridad
- PA04 Evaluar amenazas
- PA05 Evaluar la vulnerabilidad
- PA06 Construir argumentos de aseguramiento
- PA07 Coordinar la seguridad
- PA08 Monitorear la postura de seguridad
- PA09 Proporcionar entrada de seguridad
- PA10 Especificar las necesidades de seguridad
- PA11 Verificar y validar la seguridad

El SSE-CMM también incluye once áreas de proceso relacionadas con las prácticas organizativas y de proyectos. Estas áreas de proceso fueron adaptadas de la SE-CMM y se enumeran a continuación:

- PA12 - Asegurar la calidad
- PA13 - Gestionar la configuración
- PA14 - Gestionar riesgo de proyectos
- PA15 - Supervisar y controlar el esfuerzo técnico
- PA16 - Planificar esfuerzo técnico
- PA17 - Definir sistemas de Ingeniería de Procesos de la Organización
- PA18 - Mejorar los sistemas de Ingeniería de Procesos de la Organización
- PA19 - Administrar Línea de evolución del Producto
- PA20 - Gestionar el soporte del entorno de Ingeniería de Sistemas
- PA21 - Proporcionar las habilidades y conocimiento actuales
- PA22 - Coordinar con los proveedores

Las prácticas genéricas

Prácticas genéricas son las actividades que se aplican a todos los procesos. Abordan los aspectos de gestión, medición y la institucionalización de un proceso. En general, se utilizan durante una evaluación para determinar la capacidad de una organización para llevar a cabo un proceso.

Prácticas genéricas se agrupan en áreas lógicas llamadas "Características comunes" que se organizan en cinco "niveles de capacidad", que representan el aumento de la capacidad organizativa. A diferencia de las prácticas básicas de la dimensión de dominio, las prácticas genéricas de la dimensión de capacidad están ordenadas de acuerdo a la madurez. Por lo tanto, las prácticas genéricas que indican niveles más altos de la capacidad del proceso se encuentran en la parte superior de la dimensión de capacidad.

Las características comunes están diseñadas para describir grandes cambios en forma característica de una organización desarrollando procesos de trabajo (en este caso, el dominio de la ingeniería de seguridad). Cada característica común tiene una o más prácticas genéricas. La característica común más bajo es “Bases prácticas y desarrollo”. Esta característica común simplemente comprueba si una organización realiza todas las prácticas de base en un área de proceso.

Subsecuentemente características comunes tienen prácticas genéricas que ayudan a determinar qué tan bien maneja un proyecto y mejora cada área de proceso en su conjunto. La tabla 1 enumera algunos principios capturados en las prácticas genéricas.

Principio	Cómo se expresa en SSE-CMM
Tienes que hacerlo antes de que puedas manejarlo	El nivel Informalmente Realizado centra en si una organización realiza un proceso que incorpora las prácticas de base.
Entender lo que está sucediendo en el proyecto (¡donde los productos están!) Antes de definir los procesos de toda la organización.	El nivel de Planificación y bajo seguimiento se centra en cuestiones de definición a nivel de proyecto, planificación y rendimiento.
Utilice lo mejor de lo que ha aprendido de sus	El nivel bien definido se centra en la adaptación

Principio	Cómo se expresa en SSE-CMM
proyectos para crear procesos de toda la organización.	disciplinada de procesos definidos en el nivel de organización.
Usted no se puede medir hasta que sepa lo que "esto" es.	Si bien es esencial para empezar a recoger y utilizar medidas básicas del proyecto inicial (es decir, en el de Planificación y el nivel de cadenas). Medición y uso de los datos no se espera que toda la organización hasta que estén bien definidos y en particular los niveles cuantitativamente controlados han sido alcanzados
Una cultura de mejora continua requiere una base de la práctica de una buena gestión, procesos definidos y metas mensurables.	El nivel de ganancias de la mejora continua apalanca desde todas las mejoras prácticas de gestión observada en los niveles anteriores, a continuación, enfatiza los cambios culturales que sostendrán los logros alcanzados.

Tabla 1. Principales dimensiones de capacidad.

Las características comunes a continuación representan los atributos de ingeniería de seguridad madura necesarias para alcanzar cada nivel.

Nivel 1:

1.1 Prácticas Base son realizadas

Nivel 2:

2. 1 Planificación del desempeño

2.2 Desempeño disciplinado

2.3 Verificación de Desempeño

2.4 Seguimiento del desempeño

Nivel 3:

3.1 Definición de un proceso estándar

3.2 Realizar el proceso definido

3.3 Coordinar el proceso

Nivel 4:

4.1 El establecimiento de los objetivos medibles de calidad

4.2 Gestión objetivamente del desempeño

Nivel 5:

5.1 Mejora de la Capacidad Organizacional

5.2 Mejora de la efectividad del proceso

El SSE-CMM también no implica requisitos específicos para la realización de las prácticas genéricas. Una organización es generalmente libre de planificar, seguir, definir, controlar y mejorar sus procesos de cualquier manera o secuencia que elijan. Sin embargo, debido a que algunas prácticas genéricas de nivel superior dependen de prácticas genéricas de menor nivel, se alienta a las organizaciones a trabajar en las prácticas genéricas de menor nivel antes de intentar alcanzar los niveles más altos.

Los niveles de capacidad

Hay más de una forma de prácticas de grupo en las características comunes y rasgos comunes en los niveles de capacidad. La siguiente discusión se dirige a estas características comunes.

El ordenamiento de las características comunes se deriva de la observación de que la implementación e institucionalización de algunas prácticas se benefician de la presencia de otros. Esto es especialmente cierto si las prácticas están bien establecidas. Antes de que una organización pueda definir, realizar y utilizar un proceso eficaz, cada proyecto debería tener un poco de experiencia manejando la ejecución de dicho proceso. Antes de la institucionalización de un proceso de estimación específica para toda una organización, por ejemplo, una organización debería primero tratar de utilizar el proceso de estimación en un proyecto. Sin embargo, algunos aspectos de la aplicación de procesos y la institucionalización deben ser considerados en conjunto (no uno solicitado antes de la otra), ya que trabajan juntos para mejorar la capacidad.

Características comunes y niveles de capacidad son importantes, tanto en la realización de una evaluación y mejora de la capacidad de proceso de la organización. En el caso de una evaluación cuando un organismo tenga algunos, pero no todos los rasgos comunes implementados a nivel de capacidad particular para un proceso en particular, la organización por lo general opera en el nivel de capacidad completada más bajo para ese proceso. Por ejemplo, una organización que lleva a cabo todo menos uno de los de nivel 2 de prácticas genéricas para alguna zona proceso debe recibir una calificación de Nivel 1. Una organización no puede obtener el máximo beneficio de haber implementado una característica común si está en su lugar, pero no todas las características comunes a los niveles de capacidad más bajos. Un equipo de evaluación debe tener esto en cuenta en la evaluación de los procesos individuales de una organización.

En el caso de la mejora, la organización de las prácticas en los niveles de capacidad ofrece una organización con una "hoja de ruta de mejora," en caso de que el deseo de mejorar su capacidad para un proceso específico. Por estas razones, las prácticas en el SSE-CMM se agrupan en características comunes, que están ordenados por niveles de capacidad.

La evaluación se debe realizar para determinar los niveles de capacidad para cada una de las áreas de proceso. Esto significa que se puede y probablemente existirán diferentes áreas de proceso en los diferentes niveles de capacidad (ver figura 7). La organización podrá entonces utilizar esta información específica del proceso como un medio para centrarse en mejorar sus procesos. La prioridad y secuencia de actividades de la organización para mejorar sus procesos deben tener en cuenta sus objetivos de negocio.

Objetivos de la empresa son el principal impulsor en la interpretación de un modelo como el SSE-CMM. Pero, hay un orden fundamental de las actividades y los principios básicos que impulsan la secuencia lógica de los esfuerzos típicos de mejora. Este orden de las actividades se expresa en las características comunes y las prácticas genéricas del lado del nivel de capacidad de la arquitectura SSE-CMM.

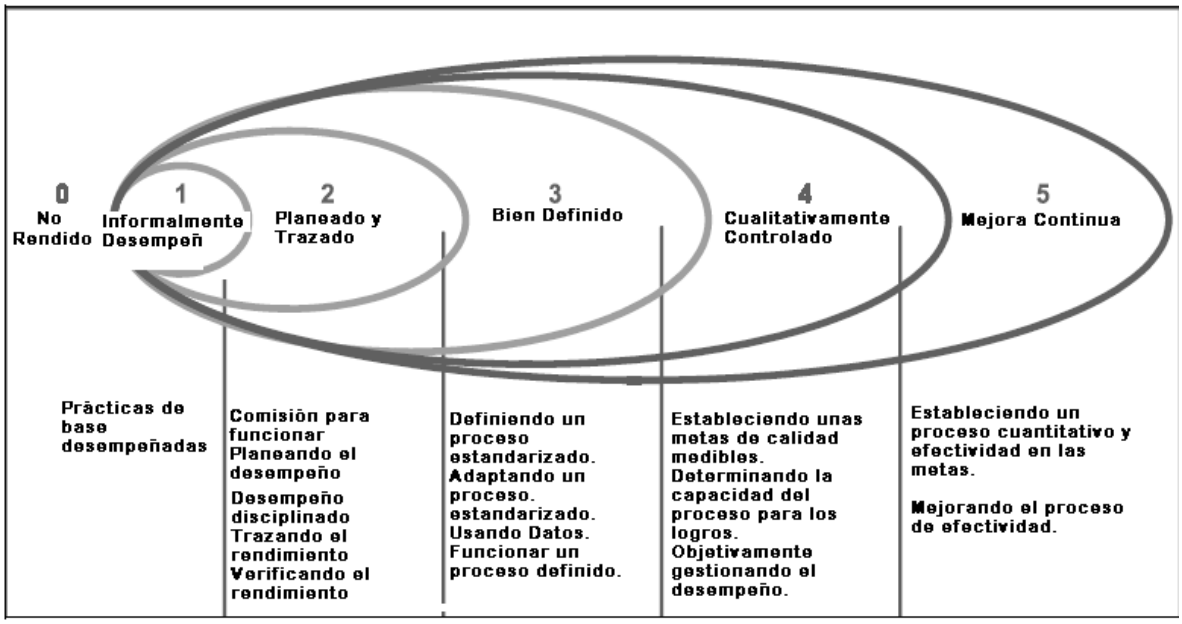


Figura 7 – Niveles de Capacidad representan la madurez de las organizaciones de ingeniería de seguridad.

Dimensión capacidad / Mapeo del marco de medición.

En el caso de la SSE-CMM la dimensión capacidad está organizada en una serie de "niveles de capacidad". Cada nivel de capacidad se compone de una serie de "características comunes", que a su vez se componen de uno o más "prácticas genéricas".

Prácticas Base de Seguridad

Esta cláusula contiene las prácticas base, es decir, las prácticas que se consideran esenciales para la realización de la ingeniería básica de seguridad. Tenga en cuenta que las áreas de proceso se numeran sin ningún orden en particular desde el SSE-CMM no prescribe un proceso o secuencia específica.

Una organización puede evaluarse comparándolo con cualquier área de un solo proceso o combinación de áreas de proceso. Las áreas de proceso juntos, sin embargo, están destinadas a cubrir todas las prácticas de base para la ingeniería de seguridad y hay muchas interrelaciones entre las áreas de proceso. En la actualidad, la SSE-CMM comprende 11 áreas de proceso de seguridad, cada uno de los cuales contiene una serie de prácticas de base. Cada área de proceso se identifica en los apartados siguientes.

El formato general de las áreas de proceso se muestra en la Figura 8. La descripción resumen contiene una breve descripción de la finalidad del área de proceso. Cada área de proceso se descompone en un conjunto de prácticas de base. Las prácticas base se consideran elementos obligatorios (es decir, deben ser implementadas con éxito para lograr el propósito

del área de proceso que apoyan). Cada práctica de base se describe en detalle siguiendo el resumen del área de proceso. Los objetivos identifican el resultado final deseado de la implementación del área de proceso.

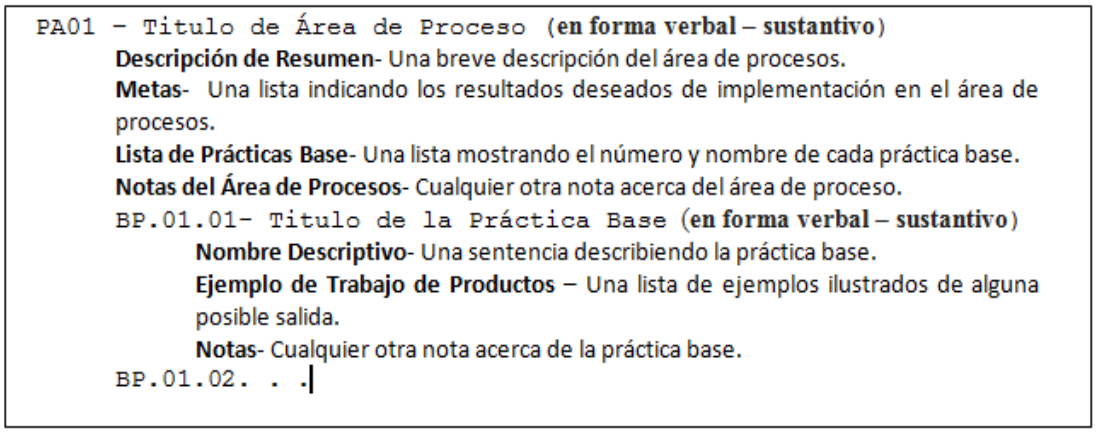


Figura 8. Formato de área de proceso.

2.3.2 Program Review for Information Security Management Assistance (PRISMA) (Bowen & Kissel, 2007)

Introducción

Este Informe proporciona una visión general del NIST de Programa de Revisión de Asistencia para la gestión de la Seguridad de la Información metodológica (PRISMA). La metodología PRISMA es un medio de emplear un enfoque estandarizado para examinar y medir la postura de seguridad de la información de un programa de seguridad de la información. Por lo tanto, PRISMA se emplea normalmente por personal de seguridad de la información, los colaboradores internos, partes independientes, auditores e Inspectoría General (IG) del personal asesor.

Objetivos

- Identificar información sobre deficiencias de los programas de seguridad.
- Establecer una línea base del programa de seguridad para medir la mejora futura siguiendo personal clave o cambios organizativos.
- Validar la finalización de las acciones correctivas o la postura de seguridad de la información del programa.
- Proporcionar información de apoyo para la tabla de puntuación de la Gestión de la Seguridad de la información Federal (FISMA) e informar.
- Preparar a favor o en efectuar una estimación, evaluación, o una revisión de un programa de seguridad de la información.

Los puntos anteriores se consolidan en los objetivos principales de PRISMA, que son:

- Ayudar a las agencias a mejorar la seguridad / protección de la información federal y Tecnología de la Información (TI) y sus componentes relacionados entre sí (incluyendo contratistas, los gobiernos estatales y locales que actúan en nombre de las organizaciones federales).
- Ayudar a reducir la interrupción de las operaciones y los activos federales críticos.

- Mejorar la agencia federal de protección de infraestructuras críticas (PIC), los esfuerzos de planificación y ejecución.
- Apoyar la implementación de marcos y estrategias de seguridad de la información más sistemática, basada en el riesgo y costo-efectividad.

Una salida de PRISMA es un sistema de puntuación basado en la madurez que se centra en nueve (9) áreas temáticas de revisión primaria (Tas) de seguridad de la información (véase la Tabla 2). Esta salida proporciona una gestión ejecutiva con una clara indicación de la postura de seguridad de la información del programa de seguridad de la información de la agencia que se puede utilizar para la toma de decisiones ejecutivas.

AT	Áreas de Gestión, Operacional y Técnica	Política	Procedimiento	Implementado	Probado	Integrado
1	Gestión de la Seguridad de la información y Cultura	0.63	0.60	0.30		
2	Planeación de la Seguridad de la Información	0.20	0.20			
3	Concientización, entrenamiento y Educación de Seguridad		0.65	0.37	0.31	
4	Presupuestos y Recursos		0.40	0.20		
5	Gestión de Ciclo de Vida					
6	Certificación y Acreditación	0.80	0.30			
7	Protección a Infraestructura Crítica		0.60	0.30		
8	Respuesta a Incidente y Emergencia	0.80	0.50			
9	Controles de Seguridad	0.80	0.60	0.60		

Tabla 2. Nueve Áreas temáticas (TA) donde muestra el nivel de madurez de la revisión de los resultados.

Cada TA anterior consiste en subtemas de áreas (STA: no se muestran en la Tabla 2) y cada STA consiste en un número de criterios. El primero de ocho (8) TA se centra en los aspectos estratégicos de la gestión del programa de seguridad de información. La revisión identifica el nivel de madurez del programa de seguridad de la información y la capacidad de la organización para cumplir con los requisitos vigentes en ocho áreas. La última TA revisa los aspectos técnicos del programa general de seguridad de la información. Por lo tanto, PRISMA proporciona un marco para ayudar a los propósitos de instrucción, así como para ayudar a evaluar, estudios independientes, o revisiones.

Descripción de PRISMA

La metodología PRISMA fue empleada con éxito en varias revisiones independientes de la madurez de seguridad de la información de los diversos programas de la agencia federal en los últimos cinco años. La metodología es un proceso escalable y probado con éxito y un enfoque para evaluar el programa de seguridad de la información de una organización. Simplemente empleando los enfoques metódicos aumenta la conciencia de seguridad de la información del personal de seguridad, los entrevistados y personal de la agencia. En el otro extremo de la escala,

PRISMA identifica las acciones correctivas del programa de seguridad y de manera concisa, que, si se aplican, pueden mejorar el programa de seguridad global.

La estructura de una revisión PRISMA está basado en el SEI precedente de CMM, donde el avance del desarrollo de una organización es medido por uno de los cinco niveles de madurez. Este enfoque fue incorporado en el Marco de Evaluación de Seguridad de Tecnología de Información del Consejo Federal CIO de 2000 y PRISMA, que también emplean cinco niveles de madurez en el quinto nivel de madurez representa el nivel de desarrollo más alto del programa de seguridad de la información. Los niveles se enumeran en el aumento de la madurez como sigue.

- Nivel de madurez 1: Políticas
- Nivel de madurez 2: Procedimientos
- Nivel de Madurez 3: Implementación
- Nivel de Madurez 4: Pruebas
- Nivel de Madurez 5: Integración

En el nivel de madurez inicial de desarrollo de PRISMA, la revisión determina la existencia de "políticas" actuales, seguridad de la información documentada en el programa federal de seguridad de la información. El segundo nivel de madurez PRISMA revisa la existencia de documentados «procedimientos» desarrollados a partir de las políticas. El tercer nivel de madurez PRISMA revisa la «ejecución» de las políticas y procedimientos. Cuarto nivel de madurez de PRISMA revisa la «prueba» de la aplicación de las políticas y procedimientos de seguridad de la información. El nivel de madurez PRISMA más alta, revisa el programa o agencia para (1) las políticas de seguridad de la información «integración» de los últimos cuatro niveles de madurez, es decir, (2) procedimientos, (3) la implementación y (4) la prueba. Un programa u organización sólo pueden alcanzar un mayor nivel de madurez después de alcanzar el nivel de madurez anterior. Por ejemplo, si un programa de seguridad de la información demuestra que cumplieron con los criterios de asistencia técnica a un nivel de madurez de tres (aplicación), pero no satisface los criterios de asistencia técnica para el nivel de madurez de una (política), entonces el programa de seguridad de la información no alcanzó el nivel de madurez tres. 'Política' es lo que define la línea base que todos los niveles de actividad y de vencimientos posteriores que deben demostrar el cumplimiento y la coherencia.

AT	Áreas de Gestión, Operacional y Técnica	Política	Procedimiento	Implementado	Probado	Integrado
1	Gestión de la Seguridad de la información y Cultura	0.63	0.60	0.30		
2	Planeación de la Seguridad de la Información	0.20	0.20			
3	Concientización, entrenamiento y Educación		0.65	0.37	0.31	

STA	Titulo					
3.1	Concientización, Entrenamiento y Educación de Seguridad					
3.1	1. ¿Tiene empleados y contratistas recibiendo adecuado entrenamiento para llenar sus responsabilidades de seguridad previamente del sistema?	Pregunta de la Madurez de Política	Pregunta de la Madurez de Procedimientos	Pregunta de la Madurez en Implementación	Pregunta de la Madurez en Prueba	Pregunta de la Madurez en Integración
3.1	2. ¿Está el entrenamiento de seguridad de la información y desarrollo profesional documentado y monitoreado por el personal?	Pregunta de la Madurez de Política	Pregunta de la Madurez de Procedimientos	Pregunta de la Madurez en Implementación	Pregunta de la Madurez en Prueba	Pregunta de la Madurez en Integración

4	Presupuestos y Recursos		0.40	0.20		
5	Gestión de Ciclo de Vida					
6	Certificación y Acreditación	0.80	0.30			
7	Protección a Infraestructura Crítica		0.60	0.30		
8	Respuesta a Incidente y Emergencia	0.80	0.50			
9	Controles de Seguridad	0.80	0.60	0.60		

Tabla 3. Muestra una vista más cercana de algunas tareas y sub tareas

Restricciones y suposiciones de PRISMA.

Una revisión PRISMA puede estar unida por varias restricciones y suposiciones. Para ejemplos, una revisión PRISMA:

- Utiliza la información agencia / programa existente para determinar el estado del programa de seguridad actual.
- ¿Es una "instantánea en el tiempo" y sólo tiene en cuenta los datos históricos y los datos disponibles en el momento en que la revisión PRISMA se lleva a cabo.
- ¿Es subjetiva utilizando una metodología definida y asume que todos los datos de la entrevista son válidos y correctos?
- ¿Es una revisión a nivel de gestión de detalle personalizable para lograr objetivos o directrices definidas?
- Se basa en "material de muestra limitado" proporcionando al equipo de revisión de PRISMA. Cuando se ha recibido más información, la opinión se convierte en una mejor postura del panorama de seguridad de la información de la agencia que evalúa.
- La revisión ayudará a la certificación y acreditación (C & A) del proceso, pero no tomara el lugar del proceso de la C & A desde una revisión PRISMA, se centra en el programa de seguridad.
- Es ejecutado por individuos con conocimientos de FISMA, estándares NIST y asesoría, y programas de seguridad.

- Es un proceso estandarizado para la recolección y la calificación de la información, pero requiere de un análisis por miembros del equipo de PRISMA.

Audiencia

La audiencia de este documento incluye:

- El personal de gestión con un rol en la seguridad de la información a nivel del programa de seguridad de información.
- Personal de Seguridad de la Información.
- Los revisores internos.
- Las partes independientes.
- Cuentas, (internos y externos).
- Personal asesor Inspector General.

Enfoque General de PRISMA

Una revisión PRISMA se centra en parte o la totalidad de los aspectos estratégicos y técnicos de un programa de seguridad de la información. La revisión identifica el nivel de madurez del programa de seguridad de la información y la capacidad de la agencia u organización para cumplir con los requisitos existentes en las siguientes nueve (9) Áreas temáticas (TA):

1. Gestión de la Seguridad y la Cultura

2. Planificación de la Seguridad de la Información

3. Conciencia de Seguridad, Formación y Educación

4. Presupuesto y Recursos

5. Gestión del Ciclo de Vida

6. Certificación y Acreditación

7. Protección de Infraestructuras Críticas

8. Respuestas a Incidentes y Emergencias

9. Controles de seguridad

La revisión PRISMA se basa en cinco niveles de madurez: la política, procedimientos, implementación, prueba, y la integración. Una breve descripción de cada nivel se proporciona en la Tabla 4. El equipo de revisión PRISMA evalúa el nivel de madurez de cada uno de los criterios de revisión. Un mayor nivel de madurez sólo se puede lograr si se alcanza el nivel de madurez anterior. Por lo tanto, si una política no está documentada por un criterio específico, ninguno de los niveles de madurez se alcanza para ese criterio específico.

Descripción de los niveles de madurez PRISMA
Nivel de madurez 1: Políticas • Formal, hasta la fecha políticas documentadas declarados como "será" o "sería" existen declaraciones y están fácilmente disponibles para los empleados. • Las políticas establecen un ciclo continuo de evaluación de riesgos, la aplicación y utiliza el monitoreo de la efectividad del programa. • Las políticas se escriben para cubrir todas las instalaciones y operaciones de la agencia o de un activo

Descripción de los niveles de madurez PRISMA
específico. • Las políticas son aprobadas por las principales partes afectadas. • Las políticas delinean la estructura de gestión de seguridad de la información, asignando claramente las responsabilidades de seguridad de la información, y sentar las bases necesarias para medir de forma fiable el progreso y el cumplimiento. • Políticas identifican sanciones específicas y acciones disciplinarias que deben utilizarse si la política no es seguida.
Nivel de madurez 2: Procedimientos • Formal, hasta a la fecha, los procedimientos documentados se proporcionan para aplicar los controles de seguridad identificadas por las políticas definidas. • Procedimientos claros donde el procedimiento se va a realizar, cómo el procedimiento se va a realizar, cuando el procedimiento se va a realizar, quien llevara a cabo el procedimiento y que el procedimiento va a realizar. • Procedimientos definen claramente las responsabilidades de seguridad de la información y los comportamientos esperados para (1) Propietarios de activos y usuarios, (2) el personal de gestión y datos de recursos de procesamiento de información, (3) de gestión y (4) los administradores de seguridad de la información. • Procedimientos contienen individuos apropiados para ser contactados para obtener más información, orientación y cumplimiento. • Procedimientos documentan la aplicación y el rigor en la que se aplica el control.
Nivel de Madurez 3: Implementación • Los procedimientos son comunicados a las personas que están obligados a seguirlos. • Procedimientos y controles de seguridad de la información se aplican de manera consistente en todas partes que se aplica el procedimiento y se refuerzan a través de la formación. • Enfoques ad hoc que tienden a aplicarse de forma individual • La prueba inicial se lleva a cabo para garantizar los controles funcionen según lo previsto.
Nivel de Madurez 4: Prueba • Las pruebas se realizan de forma rutinaria para evaluar la adecuación y eficacia de todas las implementaciones. • Pruebas que garantizan que todas las políticas, procedimientos y controles están actuando según lo previsto y que garantizan el nivel de seguridad de la información apropiada. • Se toman medidas correctivas eficaces para subsanar las deficiencias detectadas, incluidas las identificadas como resultado de los incidentes de seguridad potencial o real de información o a través de las alertas de seguridad de información emitidas por US-CERT, los vendedores, y otras fuentes de confianza. • Las autoevaluaciones, un tipo de prueba que se puede realizar por personal de la agencia, por los contratistas, u otros dedicados por administración de la agencia, se llevan a cabo de forma rutinaria para evaluar la adecuación y eficacia de todas las implementaciones. • Las auditorías independientes tales como las dispuestas por la Oficina de Responsabilidad Gubernamental (ORG) o una agencia de Inspectoría General (IG), son un importante control sobre el desempeño de las agencias, pero no deben ser vistos como un sustituto de las evaluaciones iniciadas por la gestión de la agencia. • La información obtenida de los registros de incidentes potenciales y reales de seguridad de la información y de las alertas de seguridad, tales como los emitidos por los proveedores de software se consideran como resultados de las pruebas. Dicha información puede identificar vulnerabilidades específicas y proporciona una visión de las últimas amenazas y el riesgo resultante. • Requisitos de evaluación, incluidos los requisitos sobre el tipo y frecuencia de las pruebas, están documentados, aprobados y aplicados efectivamente. • La frecuencia y el rigor con el que se ponen a prueba los controles individuales dependen de los riesgos que se plantean si los controles no funcionan con eficacia.
Nivel de Madurez 5: Integración • Aplicación efectiva de los controles de seguridad de la información

Descripción de los niveles de madurez PRISMA
• Las políticas, los procedimientos, las implementaciones y pruebas son continuamente revisados y se hacen mejoras. • Seguridad de la información en integración en la Planificación de Capital y Control de Inversiones (CPCI). • Un programa de seguridad de la información completa es una parte integral de la cultura organizacional. • La toma de decisiones se basa en el precio, el riesgo y el impacto de la misión. • La consideración de seguridad de la información es omnipresente en la cultura. • Un programa de seguridad de la información en toda la empresa activa logra seguridad de la información económica. • Seguridad de la información es una práctica integrada. • Se comprenden y gestionan las vulnerabilidades de seguridad. • Las amenazas son continuamente reevaluadas y los controles adaptados a las cambiantes condiciones de seguridad de la información. • Alternativas de seguridad de la información rentables son identificados cuando surja la necesidad. • Costos y beneficios de la seguridad de la información se miden con la mayor precisión posible y • Métricas de estado para el programa de seguridad de la información, así como medidas de rendimiento de las inversiones de seguridad de información CPCI individuales se establecen y se consolidan.

Tabla 4. Descripción de los niveles de madurez PRISMA

Ventajas del PRISMA

- Utiliza niveles de madurez para evaluar
- Revisa el nivel de gestión, no específicamente la parte técnica
- Utiliza la información proporcionada por los propietarios del sistema, con el uso de entrevistas y el uso de muestras limitadas para efecto de tener información de confianza
- Proporciona un metodología para la realización de un revisión
- Utiliza los niveles de madurez basados en CMM
- Proporciona una metodología para la realización de una revisión

Descripción de la Arquitectura PRISMA.

Figura 9 es un resumen de un flujo de proceso para una revisión general PRISMA. Los primeros cuatro (4) pasos representan las actividades de preparación, mientras que el resto de pasos proporcionan orientación sobre la ejecución de una revisión efectiva en el ámbito definido. Las fases de preparación y ejecución PRISMA se detallan en las secciones siguientes.

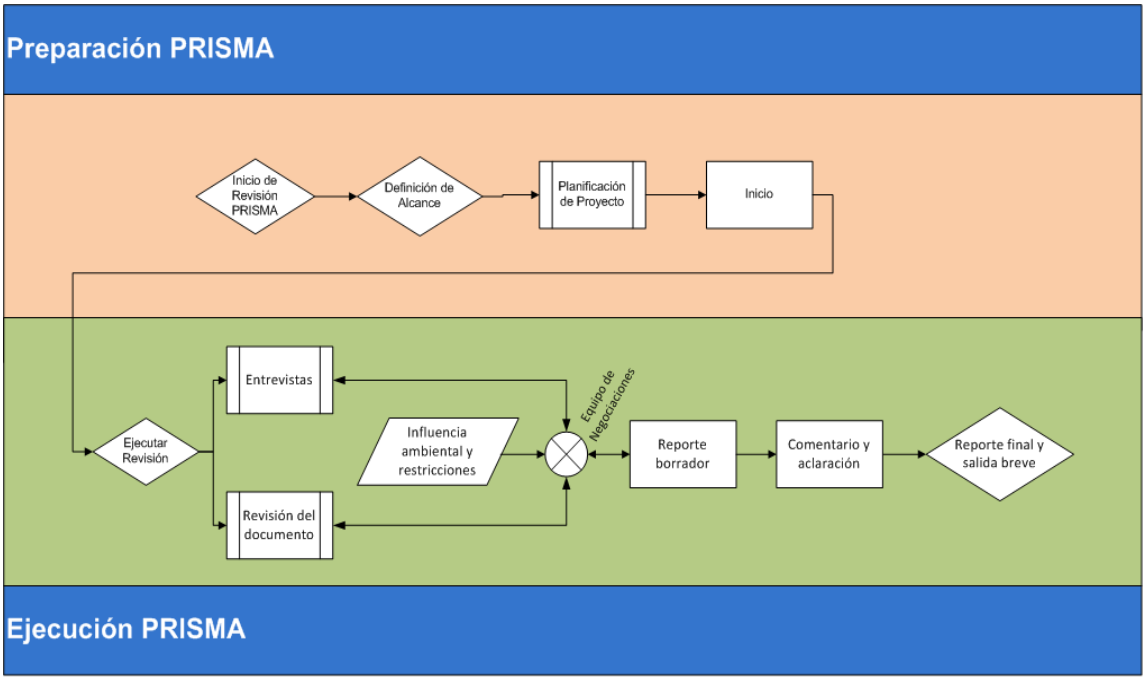
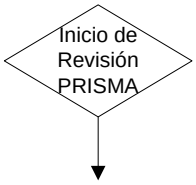
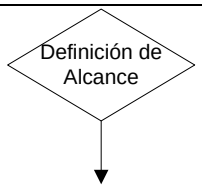


Figura 9. Descripción general del proceso PRISMA

Preparación PRISMA

En esta sección se ofrece un enfoque y plantillas sugeridas para planificar y preparar una revisión PRISMA. La revisión, sin embargo, se puede escalar según sea necesario para el programa de seguridad de información. El enfoque tal como se muestra en la Figura 9 es el mismo independientemente de adaptar o escalar. La Tabla 5 presenta un resumen de las actividades y resultados de la Fase de Preparación.

Pasos de Proceso Prisma	Acciones	Salidas
	• Definir "Necesidad" de gestión para llevar a cabo una revisión PRISMA	• Objetivos de Revisión PRISMA • Liderar y Brindar Soporte a organizaciones • Restricciones y Supuestos • Nivel de Endoso para Gestión Apropiada y autoridad para aplicar recursos organizacionales
	• Seleccionar Alcance – Determinar o demostrar la capacidad de gestión de seguridad de la información para: ○ Total de Agencias ○ Nivel de Programa ○ Áreas Temáticas ○ Nivel de Madurez	• Declaración de Alcance de Revisión PRISMA • Entregables de Proyecto

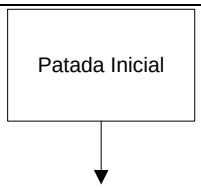
Pasos de Proceso Prisma	Acciones	Salidas
	• Planificación de Recursos • Determinar Hitos de Horario • Identificar roles y personal clave participante; notificar al personal clave • Preparar/Seleccionar criterio PRISMA • Identificar la información aplicable de la revisión • Responder a una agencia genérica / Programar cuestionarios	• Plan de Proyecto • Contratar SOW, si es necesario • Lista de Contacto de Personal Clave • Memorándum para el personal clave de la entrevistas PRISMA [Apéndice B] • Documento de lista de revisión [Apéndice D y F] • Completar Cuestionarios Genéricos [Apéndice E]
	• Presentar alcance y objetivo • Presentar programación y Enfoque PRISMA a los participantes de la Revisión	• Presentación para el equipo de revisión, brindar soporte y gestión

Tabla 5. Las actividades de preparación PRISMA

Paso 1: Iniciación de Revisión PRISMA

El paso Iniciación de Revisión PRISMA establece el fundamento o la "necesidad" de la revisión. La "necesidad" de la organización variará de forma única con la organización y adaptación a cualquier período de tiempo, sin embargo, pueden incluir:

- Determinación de las brechas de los programas de seguridad de la información
- Determinar programas / niveles de madurez
- Validación independiente del programa / programa de agencia de sistema de seguridad de la de información, como la estimación, evaluación o de revisión y
- Una auditoría o inspección exigida por el capítulo, la autoridad superior u otro mandato

A continuación, un objetivo o grupo de objetivos se desarrollan en base a la declaración de "necesidad" y pueden incluir:

- Identificar las deficiencias del programa de seguridad
- El establecimiento de un programa de seguridad de línea base para medir el crecimiento futuro siguiendo personal clave o cambios organizativos
- Justificar la ayuda presupuestaria continua para un programa de seguridad de la información en particular
- La validación independiente del "estado del programa"
- Información complementaria sobre el cuadro de mando FISMA y
- Preparación para la realización de una revisión o Inspectoría General

La revisión PRISMA "Necesita" y subsecuentemente declara los objetivos ha desarrollar con o por el nivel de gestión organizativa adecuada con la autoridad para llevar a cabo la revisión y aplicar los recursos necesarios. Después de la captura de la "necesidad" y codificar una declaración de objetivos de la revisión, la organización principal y el director del proyecto es nombrado junto con todas las organizaciones de apoyo. Como resultado final de esta actividad, la apropiada aprobación del nivel de gestión de la revisión PRISMA es crucial para el éxito de la revisión. Este respaldo en forma de un memorando o correo electrónico autoriza formalmente la Revisión PRISMA, logrando satisfacer las necesidades y los objetivos de la organización y designa el liderazgo de revisión PRISMA y el equipo.

Paso 2: Delimitación del Alcance de Revisión PRISMA.

Como se dijo anteriormente, el proceso de PRISMA evalúa la madurez y eficacia de un programa de seguridad de la información. La construcción del proceso de PRISMA permite establecer el ámbito del proyecto de apoyo a una variedad de necesidades de la organización. La revisión PRISMA puede realizarse para un programa de seguridad de la agencia o división operativa con un enfoque en los nueve TAs o cualquier subconjunto. Además, una revisión puede ser enfocada hacia la evaluación de un nivel de madurez en particular, por ejemplo, el estado del nivel de madurez de la política.

Paso 3: Planificación del Proyecto PRISMA

Esta etapa del proceso se ocupa principalmente de la planificación de recursos y el calendario para ejecutar la revisión y el establecimiento de las bases iniciales para prepararse para las revisiones. Existen los centros de recursos iniciales para interrogación sobre los recursos humanos y de capital para ejecución y luego proceder a la revisión que se llevara a cabo en la empresa, a través de acciones contratadas o por un equipo de Inspectoría General. Otro factor a considerar es la conveniencia de una revisión internamente frente a un agente independiente con respecto a la intermediación y la presentación de observaciones. Si un agente independiente, no gubernamental es necesario, una salida principal en esta etapa es una declaración de contrato de trabajo (SOW) con las tareas PRISMA apropiadas y resultados indicados.

La planificación de la acción secundaria es preparar para las propias revisiones PRISMA mediante la identificación de contactos de personales clave principales y alternativas, la documentación de apoyo en función del alcance definido. Una lista recomendada de los principales candidatos de la entrevista personal se proporciona en la Tabla 6. Se recomienda un Memorando desde un Gerente organizacionalmente apropiado (como el CIO) para notificar y comprometer a los entrevistados PRISMA.

Lista recomendada de los principales candidatos de la entrevista personal	
Director de Información	Gerentes de Contrato
Director Financiero	Gerentes de Recursos Humanos
Director de Tecnología	Gerentes de Áreas Funcionales
Oficial Mayor de Seguridad de la Información	Gerentes de Programa
Inspector General	Oficiales de Contratación de Programas
Gerente de Seguridad de Sistemas de Información / Oficiales de Seguridad de Sistemas de Información	Representantes Técnicos de Contratación de Programas

Lista recomendada de los principales candidatos de la entrevista personal	
Autoridad de Aprobación Designada / Oficiales de Autorización	Administradores de Sistemas / Redes / Base de Datos
Gerentes de Instalaciones / Gerentes de Seguridad Física	Desarrolladores TI / o Integradores
Directores (TI, Áreas de Negocio, etc.)	Usuarios Finales

Tabla 6. Lista de Contacto Solicitado de Personal Clave.

El equipo de revisión PRISMA trabaja con el personal del programa de seguridad de información para asegurar el muestreo de personal clave sea suficiente para hacer frente a las responsabilidades del trabajo y la estructura organizativa. Documentos que apoyan la revisión deben ser catalogados según el título y la fecha de lanzamiento oficial y / o proyecto de distribución.

Durante esta actividad, el personal clave de la seguridad de la información u otros representantes de las agencias del programa de seguridad de la información bajo revisión deben completar las preguntas pertinentes del cuestionario genérico. Preguntas de apoyo al alcance y el nivel de la revisión debe seguir siendo el objetivo; Sin embargo, muchas de estas preguntas están diseñadas para proporcionar un valioso apoyo ambiental y cultural para la revisión.

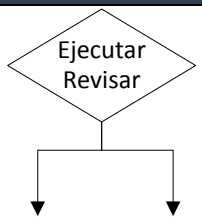
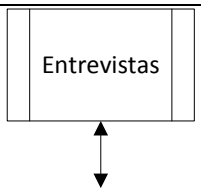
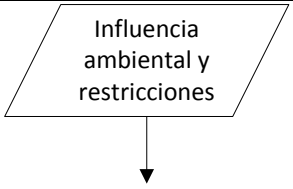
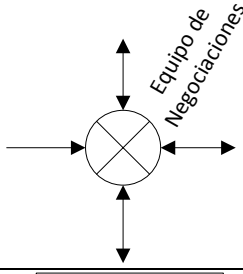
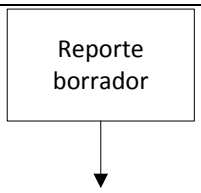
Paso 4: PRISMA reunión inicial

Se recomienda una reunión inicial entre la parte implementadora PRISMA (personal de seguridad de la información, los auditores, inspectores, etc.) y los representantes del programa de seguridad de la información en revisión. En la reunión, el objetivo identificado, el alcance, el cronograma, los criterios de documentos, y el enfoque de entrevista relacionada se les informará a los participantes. En segundo lugar, el Memorando a nivel de gestión puede ser discutido para confirmar la información de contacto y para desarrollar un calendario con los entrevistados.

La reunión inicial también se puede utilizar con el equipo de revisión (que puede ser el personal de seguridad de la información, auditores o inspectores), así como los principales participantes de la entrevista y la gestión organizacional para la validación y solicitud de información adicional: áreas candidatas para la discusión incluyendo las respuestas al cuestionario genérico, la lista de documentación, y otros candidatos u otras entrevistas.

Ejecutar la Revisión PRISMA

Fase de ejecución de la revisión en última instancia resulta en un informe publicado y consiste en la revisión de la documentación de la agencia, entrevistas con el personal de la agencia y la realización de un análisis de las deficiencias de revisión. El equipo de revisión PRISMA lleva a cabo la revisión de una manera que minimice el impacto de la revisión de las operaciones necesarias. La Tabla 7 presenta un resumen de las actividades y resultados de ejecutar una Revisión PRISMA.

Pasos del Proceso PRISMA	Actividades	Salidas
	• Iniciar entrevistas del personal clave y la documentación en paralelo (si es práctico) • Trazar la entrevista y revisar el progreso de las métricas del documento	Completar semanalmente el progreso del estado del reporte
	• Reunir y clasificar los documentos identificados • Evaluar los documentos basados en el PRISMA el alcance de la revisión y el apoyo de los criterios del PRISMA TA • Registrar los comentarios y evaluar los resultados	• Resultados de la evaluación de documentos • Comentarios del soporte.
	• Programar las entrevistas con los individuos la lista del personal clave. • Dirigir las entrevistas al personal clave usando preguntas adaptadas de una a 1.5 horas • Registrar las respuestas de la entrevista, comentarios y evidencias de apoyo.	• Responder a partir de las preguntas de la entrevista • Comentarios del soporte y la evidencia del el sistema de información del programa de seguridad
	• Basada en la observación, identificar las influencias ambientales y las restricciones. • Determinar los asuntos relevantes, amenazas o factores culturales.	• Datos revisados de soporte.
	• Periódicamente discutir y colaborar los resultados revisados • Alcances de las recomendaciones de la discusión.	• Comentarios del soporte e información.
	• Completar el análisis de TA determinando las observaciones y recomendaciones. • Completar el reporte borrador de repaso de PRISMA.	• Reporte borrador (Apéndice G) • Observaciones y tareas • Recomendaciones • POAM&Ms propuesto. • Análisis de FISMA

Pasos del Proceso PRISMA	Actividades	Salidas
	• Suscribir el reporte borrador a los accionistas para revisión. • Revisar comentarios y preguntas; negociar con los accionistas respectivamente.	• Revisar comentarios e identificar áreas de aclaración y actualización. • Responder los comentarios y aclaraciones.
	• Incorporar nuevas observaciones y resultados a partir de comentarios y negociaciones. • Completar y distribuir el reporte de repaso del PRISMA	• Reporte de repaso del PRISMA.

Tabla 7. Presenta un resumen de las actividades y resultados de ejecutar una Revisión PRISMA

Paso 5: Revisión de Documentos.

Utilizando los criterios de revisión PRISMA, un(os) miembro (s) del equipo de revisión de PRISMA revisa todos los documentos relacionados con cada una de las áreas temáticas PRISMA dentro del alcance de la revisión y el objetivo de vencimiento del documento (es decir, un nivel de madurez de política frente a una implementación del nivel de madurez de tipo de documento). El miembro del equipo de Revisión PRISMA determina si el documento es "conforme", "parcialmente conforme", o "no conforme" cuando se evalúa con los criterios del documento PRISMA. La siguiente es una lista de elementos para recordar a la hora de revisar los documentos:

- Documentos, especialmente las políticas y procedimientos deben ser identificados como "Final" y "Aprobado" a tener en cuenta para el cumplimiento de la madurez
- Cantidad y calidad de los documentos se deben considerar, cuando sea necesario, para responder a ciertos criterios PRISMA. En otras palabras, si el programa en revisión tiene diez sistemas aplicables y el equipo de revisión PRISMA recibe sólo tres planes de seguridad que cumplen totalmente para tres de estos sistemas, el miembro del equipo de revisión PRISMA anotará los resultados como un "cumplimiento parcial", ya que siete planes de seguridad están desaparecidos

Pregunta de Nivel de Madurez	Ejemplo de respuesta de la Pregunta de Nivel de Madurez	Indicador de cumplimiento	Explicación
Nivel de Madurez 1: Política. ¿La política documentada requiere controles tales como la separación de tareas, privilegios mínimos y responsabilidad individual incorporada en todas las operaciones del negocio?	Sí, política documentada, Capítulo 6 parte 5.2, proveerá acceso a los sistemas de información de las organizaciones según la responsabilidad individual, separación de tareas, y privilegios mínimos en la práctica.	Conformidad	

Pregunta de Nivel de Madurez	Ejemplo de respuesta de la Pregunta de Nivel de Madurez	Indicador de cumplimiento	Explicación
Nivel de Madurez 2: Procedimientos. ¿Son los procedimientos documentados para incorporarlos a los controles tales como la separación de tareas, privilegios mínimos y responsabilidad individual incorporada en todas las operaciones?	Sí, Capítulo 2 parte 1.2 Los procesos de posteado de internet proveen instrucciones como: dónde, cómo, cuándo y quién incorpora los controles para la separación de tareas, menos privilegios, y responsabilidad individual por postear al internet. Este documento provee un sometimiento parcial desde que otras funciones necesitan tales procedimientos.	Conformidad Parcial	Este procedimiento aplica solamente a postear internet; otros eventos son necesariamente para proveer sujeción completa.
Nivel de Madurez 3: Implementación. ¿Son los controles tales como la separación de tareas, privilegios mínimos y responsabilidad individual incorporada en todas las operaciones de los negocios?	Sí, Sección, 3.3.1.1 provee asignación general de seguridad de la información, responsabilidades basadas en principios de separación de tareas, privilegio mínimo y responsabilidad individual. Sección 3.3.6.1 el estado del sistema "X" separado de usuarios en dos categorías primarias: Súper usuarios y usuarios. Los Súper usuarios son subdivididos en 4 tipos: AAs, revisadores EC, SAs y DBAs. Este documento provee un sometimiento parcial desde otros sistemas que requieren implementación.	Conformidad Parcial	Un sistema tiene evidencia de implementar estos controles de acceso. Sin embargo, este es solamente una obediencia parcial para las preguntas desde este documento no provee evidencia de implementación de todos los sistemas.
Nivel de Madurez 4: Examen. ¿Son los exámenes periódicamente conducidos a verificar aquellos papeles específicos y las responsabilidades son	No, No direccionado.	No Conformidad	

Pregunta de Nivel de Madurez	Ejemplo de respuesta de la Pregunta de Nivel de Madurez	Indicador de cumplimiento	Explicación
separadas y el individuo no tiene la capacidad para desempeñar estos múltiples papeles y responsabilidades?			
Nivel de Madurez 5: Integración ¿Está separando papeles y responsabilidades aceptadas y son negocios estandarizados en la práctica que no representa desafío o derrota en algún propósito?	No, no direccionado	No Conformidad	

Tabla 8 Revisión de documentos

La información de revisión de documentos no requiere corroboración por medio de entrevistas.

Paso 6: Entrevistas

Las entrevistas proporcionan información sobre seguridad de la información personalizada del programa de conocimiento de la información en la documentación, sus actitudes, etc. Para una mayor precisión en la medición de esta información, el NIST recomienda que todas las entrevistas PRISMA incluyan dos miembros del equipo de revisión para garantizar la documentación completa y la comprensión de todos los comentarios del entrevistado. Un miembro del equipo de revisión PRISMA de los horarios de las entrevistas necesarias basándose en horarios de los entrevistados y el entrevistador, tratando de programar todas las entrevistas requeridas poco después de la reunión inicial. En los casos en que una entrevista no se puede programar, se debe hacer un intento para programar horarios alternativos según lo permitido e inmediatamente poner la situación en conocimiento de la gestión de su caso para su resolución.

El equipo de revisión PRISMA debería asegurar un muestreo adecuado de entrevistas debidamente programado. Una sesión de la entrevista por lo general requiere de 45 a 60 minutos, dependiendo del nivel de participación del entrevistado y experiencia en la implementación de seguridad de información de la agencia. Los entrevistadores deben tratar de realizar la entrevista en 45 minutos a respetar el tiempo del entrevistado. Los siguientes consejos son proporcionados para el entrevistador.

- Hacer presentaciones (proporcionar nombres del entrevistador PRISMA indicando organización o patrocinador) y declarar el propósito de la entrevista

- Explicar el propósito de la revisión PRISMA y cuál es el propósito de la entrevista para identificar las fortalezas y debilidades del programa de seguridad de la información que no puede obtenerse a partir de la documentación
- Explicar la no atribución de las respuestas contenidas en los almacenes de datos y el informe final. La aplicabilidad de una política de no atribución, sin embargo, depende de la política de la agencia patrocinadora, auditor o inspector general
- No registrar cualquier nombre o entrevista asociado con las respuestas del entrevistado de ninguna manera. Una vez más, la aplicabilidad de una política de no atribución, sin embargo, depende de la política de la agencia patrocinadora, auditor o Inspector General
- Pregunte sólo las preguntas asignadas al tipo de posición del entrevistado
- Documentar todas las respuestas en los formularios de entrevista vinculados a la pregunta
- Asegúrese de cada respuesta es aplicable a la pregunta y que el entrevistador entiende la respuesta
- Pregunte si los demás deben ser entrevistados o si el equipo de revisión de PRISMA debería examinar cuestiones conexas
- Pregunte si el individuo tiene sugerencias para mejorar la seguridad de la información en la organización
- Agradecer a la persona por su tiempo y asistencia

Después de la entrevista, los dos entrevistadores documentan los resultados de la entrevista de forma independiente. Los entrevistadores luego resuelven todas las discrepancias y producen un documento exhaustivo de la entrevista tan pronto como sea posible, como a los dos días de la entrevista. La respuesta a cada pregunta de la entrevista debe ser completa, incluyendo información suficiente para hacer la pregunta obvia.

Pregunta de entrevista	Muestra de respuesta de entrevista
Usuario final: **¿Cómo y qué rango tienen las reglas generales y aceptables de comportamiento para la información del sistema o TI, los recursos que usted usa han sido convenientes para usted?** **¿Está usted consciente del uso ético de los recursos TI?**	Presentemente, como nuevos empleados que se unen a la organización son requeridos para tomar capacitación detallando las reglas de seguridad general, reglas de conducta, y el uso de la ética de los recursos TI. Este entrenamiento requiere verificación a través de un examen y es repetido anualmente. Además cada vez yo cargo, y estoy presentado con un recordador de las reglas de seguridad de conducta
Administrador: ¿Qué tipo de información de entrenamiento de seguridad (tales cómo inicial, periódica, anual, etc) es dada para los administradores y hacer que ellos estén conscientes de las responsabilidades de la seguridad de la información?	Cómo el FM (Facility Manager), yo recibo el mismo entrenamiento de seguridad como todos los empleados de la organización, no hay otras capacitaciones específicas provistas.
ISSO: ¿Es un sujeto asignado a un información de ISSO y son sus trabajos primarios o tareas adicionales documentadas? ¿Es el ISSO preparado para funcionar en las tareas del trabajo?	Sí mi cita es formal y mi trabajo es detallado en el manual de seguridad de la agencia, yo recibo capacitación ISSO provista por XXX y asistí a una industria que proveyó una capacitación vía foro el

Pregunta de entrevista	Muestra de respuesta de entrevista
	año pasado.
ISSO: ¿Están las informaciones de seguridad disponibles para la educación general y conciencia de todos los usuarios del sistema?	Sí, todos los empleados requeridos asisten a entrenamiento de conciencia de seguridad y todos los empleados son requeridos para tomar un entrenamiento anual para refrescar su conocimiento. Además la división del entrenamiento provee ítems de seguridad de presentaciones de interés mensualmente o una asistencia de voluntariado.
Personal General	Sí, la información de conciencia de seguridad es refrescada anualmente y la capacitación es dirigida.

Tabla 9. Ofrece varios ejemplos de preguntas de la entrevista y la documentación ejemplo.

Paso 7: Influencias y limitaciones ambientales

Antes y durante la revisión PRISMA, los miembros del equipo de revisión PRISMA deben identificar y rastrear las influencias y limitaciones ambientales positivas y negativas que influyen en el programa/organización de seguridad de la información. Influencias y limitaciones ambientales incluyen, pero no están limitados a lo siguiente:

- Las restricciones presupuestarias
- Limitaciones de la misión de la organización
- Orden de Corte y asuntos de gobernanza
- Las influencias culturales de organización y
- Estructura de la organización.

Paso 8: Negociaciones del equipo

Periódicamente a través de la revisión, los miembros del equipo de revisión PRISMA (si el equipo es mayor que una persona) deben reunirse para discutir el progreso y colaborar con los resultados de la revisión y las observaciones. Además, los miembros del equipo pueden iniciar discusiones con respecto a las observaciones de revisión y los enfoques de recomendación.

Paso 9: Análisis PRISMA, Generación de informes y Revisión

Con base en la información obtenida de las entrevistas y revisiones de documentos que respaldan cada TA, los miembros del equipo de revisión PRISMA determinarán subjetivamente el estado del programa de seguridad de información para cada STA, así como para la asistencia técnica en general. Además, los miembros del equipo identifican los problemas de seguridad de la información, las acciones correctivas y recomiendan un plan de acción correctiva.

Análisis de Datos PRISMA

Proceso de calificación del equipo de revisión de PRISMA se inicia en el nivel de criterio individual PRISMA donde cada criterio del documento consta de cinco preguntas de nivel de

madurez, es decir, una pregunta para evaluar el nivel de madurez política, una pregunta para el nivel de madurez procedimiento, una para el nivel de aplicación, etc. para cada criterio en una revisión de documentos, el miembro (s) del equipo comienza en el nivel de madurez más bajo (es decir, la política) para determinar el cumplimiento. Si los resultados a la pregunta madurez política para un criterio específico para todos los documentos revisados son "No compatible", la puntuación general el nivel de madurez política es "No compatible" (véase, Tabla 10, el Criterio 1 de fila). Además, todos los niveles de madurez por encima de políticas (es decir, los procedimientos, implementación, prueba y de integración) para ese criterio documento se consideran "no compatibles." Si los resultados a la pregunta madurez política para el criterio específico para algunos documentos se consideran "No compatible", pero uno o más resultados de revisión de documentos son "Parcialmente Cumplida", entonces la puntuación total madurez política para ese criterio se considera "Cumple parcialmente" (véase, Tabla 10, criterio 3 filas). Si alguno de los resultados de revisión de documentos a la cuestión política de un criterio específico es "conforme", pero otro criterio es no compatible, entonces la puntuación total madurez política para ese criterio se considera "Cumple parcialmente" (véase la Tabla 10, Criterio 2 de fila). Además, si algunas de las preguntas de madurez política de los resultados de revisión de documentos son "Parcialmente Cumplida", pero cuando revisó los documentos cubren todas las porciones necesarias de la cuestión de madurez política, el resultado global indica "Cumple parcialmente" (véase la Tabla 10 Criterio 4 fila). Tabla 10 proporciona ejemplos de cómo las diferentes respuestas de revisión de documentos se pueden agregar a cuatro puntuaciones de madurez diferentes para cuatro criterios distintos de documentos de preguntas de política.

Sub tópico de Área Preguntas de Políticas	Documento 1	Documento 2	Puntuación en Madurez de Política
Pregunta de Política Criterio 1	**No cumple**	**No cumple**	**No cumple**
Pregunta de Política Criterio 2	**Cumple**	**No cumple**	Cumple parcialmente
Pregunta de Política Criterio 3	**No cumple**	Cumple parcialmente	Cumple parcialmente
Pregunta de Política Criterio 4	Cumple parcialmente [requerimiento 1 de 2]	Cumple parcialmente [requerimiento 2 de 2]	Cumple parcialmente

Tabla 10. Ejemplos de agregación de Cumplimiento.

Los miembros del equipo de revisión PRISMA deben tener cuidado de asegurar que el material y las puntuaciones críticas "tienen sentido". Esto puede requerir el examen de documentos, hablando con otras opiniones y entrevistadores, etc. Sin embargo, cada criterio es un "requisito duro" en el que cada parte del criterio se debe cumplir para obtener crédito.

Si el resultado de una cuestión de política para un criterio determinado documento es "No compatible", entonces todos los niveles de madurez más altos (procedimientos, implementación, prueba y la integración) debe ser "No compatible". Si la respuesta a la pregunta de política para un criterio determinado documento es "Cumple parcialmente" o

"conforme", a continuación, los miembros del equipo de revisión PRISMA proceden a la pregunta procedimiento para el mismo criterio del documento. El miembro del equipo de revisión PRISMA utiliza el mismo proceso de agregación para el procedimiento, la ejecución, la prueba y las preguntas de madurez integración utilizan para agregar el resultado de preguntas en madurez de política. Tan pronto como el resultado a la pregunta nivel de madurez se considera "No compatible", los restantes niveles de madurez superior deben ser "No compatibles".

2.3.3 COBIT Process Assessment Model (PMA) usando Cobit 4.1 (ISACA, 2011)

Introducción

De acuerdo a un artículo presentado en la página de Inforc Ecuador (inforc Ecuador, 2011), desde que COBIT fue dado a conocer hace 15 años, empresas de todo el mundo lo han utilizado para evaluar y mejorar sus procesos de TI. Sin embargo, hasta ahora no existía un modelo de evaluación consistente y confiable. El nuevo COBIT Assessment Programme de ISACA, que incluye el nuevo Process Assessment Model (PAM), ofrece esta consistencia y confiabilidad para que los líderes de negocio y de TI puedan confiar en el proceso de evaluación y en la calidad de los resultados mientras maximizan el valor del negocio de sus inversiones en TI.

Después de realizar una encuesta global en el 2010 para determinar la necesidad del mercado, ISACA descubrió que el 89 por ciento de los 1,400 entrevistados expresó la necesidad de una evaluación de la capacidad de los proceso de TI que fuera rigurosa y confiable.

Según comentó Gary Baker, CA, CGEIT "*COBIT PAM brinda la base para la evaluación de los procesos de TI de una empresa con COBIT 4.1 y permite que las evaluaciones de las capacidades de los procesos soporten la mejora*". "*La evaluación se basa en evidencias para asegurar un proceso confiable, consistente y repetible en el gobierno y la administración de TI*".

El COBIT Process Assessment Model (COBIT PAM) es un modelo que, tomando como base la norma ISO/IEC 15504, está orientado a la evaluación (assessment) de procesos de TI dentro de las organizaciones.

Antecedentes

ISO/IEC 15504-4 identifica la evaluación de procesos como una actividad que puede ser desarrollada ya sea como parte de una iniciativa de mejora de procesos o como parte de un enfoque para la determinación de capacidades.

El propósito de una mejora de procesos es que continuamente se mejore la efectividad y la eficiencia de la empresa. El propósito de *una determinación de capacidades* es identificar las fortalezas, debilidades y riesgos de un proceso seleccionado con respecto a un requerimiento particular del proceso y su alineación con la necesidad del negocio.

COBIT PAM provee una metodología comprensible, lógica, repetible, confiable y robusta para evaluar la capacidad de los procesos de TI.

El programa de evaluación de COBIT (PAM) incluye (ver figura 10):

- *COBIT Process Assessment Model (PAM): Using COBIT 4.1*
- *COBIT Assessor Guide: Using COBIT 4.1*
- *COBIT Self Assessment Guide: Using COBIT 4.1*

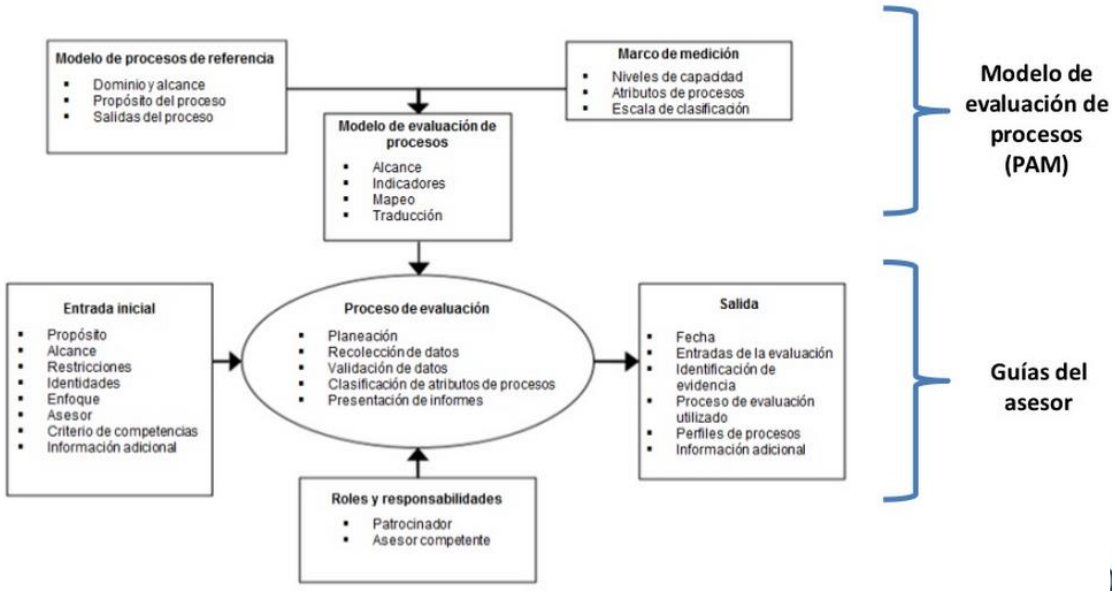


Figura 10. Modelo de evaluación de la capacidad del proceso utilizado por COBIT (PAM)

EL PAM adapta el contenido existente de COBIT 4.1 dentro de un modelo de evaluación de procesos que cumple con el estándar ISO 15504.

El programa nuevo de evaluación de COBIT es:

- Un proceso de evaluación robusto basado en ISO 15504
- Una alineación del modelo de madurez de COBIT con el estándar internacional
- Un modelo nuevo de evaluación basado en capacidades, el cual incluye:

  •Requerimientos específicos de procesos obtenidos de COBIT 4.1

  •La habilidad para lograr los atributos de los procesos basada en ISO 15504

  •La evidencia de los requerimientos

  •Requerimientos de experiencia y calificaciones por un asesor

Todo ello da como resultado una evaluación más robusta, objetiva y repetible.

Alcance Y Objetivos

COBIT Process Assessment Model (COBIT PAM) es un modelo que, tomando como base la norma ISO/IEC 15504, está orientado a la evaluación (assessment) de procesos de TI dentro de las organizaciones.

- Define el conjunto mínimo de requisitos para llevar a cabo una evaluación que asegure que los resultados son consistentes, repetibles y representativos de los procesos evaluados.
- Define la capacidad del proceso en dos dimensiones, capacidad y proceso:
  - Emplea procesos contenidos en los materiales definidos en COBIT 4.1
  - Emplea los niveles de evaluación de la capacidad y los atributos de proceso definidos en la norma ISO / IEC 15504-2
- Utiliza indicadores de capacidad de procesos y rendimiento de los procesos para determinar si los atributos de proceso se han logrado
- Mide el rendimiento del proceso a través de un conjunto de prácticas base y actividades necesarias para cumplir con los resultados del proceso, así como entradas y salidas de los productos de trabajo asociados a cada proceso
- Mide la capacidad de los procesos por el logro del atributo (escala) a través de la evidencia especifica (nivel 1) y genérica (nivel superior) de las prácticas y productos de trabajo
- Reconoce que una evaluación del proceso puede ser un motor fuerte y eficaz para la mejora de procesos.

El modelo de evaluación de proceso COBIT 4.1 apoya la realización de una evaluación, proporcionando indicadores para guiarlos sobre la interpretación de los propósitos del proceso y los resultados tal como se define en COBIT 4.1 y los atributos de proceso como se define en ISO / IEC 15504-2.

El modelo de evaluación de procesos de COBIT 4.1 se compone de un conjunto de indicadores de desempeño de los procesos y la capacidad del proceso. Los indicadores se utilizan como base para obtener la evidencia objetiva que permite a un evaluador asignar calificaciones.

Diferencias Con El Modelo Actual De Cobit

El nuevo modelo de evaluación de procesos COBIT (PAM) presenta varias diferencias con el proceso actual de COBIT 4.1, entre ellas podemos destacar:

El PAM utiliza un marco de medición que es similar en la terminología que existe con los modelos de madurez actuales de COBIT 4.1, aún y cuando las palabras son similares, las escalas *NO* son las mismas según se puede apreciar en la figura 11, como se puede observar:

- El PAM utiliza la escala de capacidades de la ISO/IEC 15504, mientras que los modelos actuales de madurez de COBIT usan una escala basada en SEI\CMM[2]
- El nivel 3 de PAM NO es el mismo nivel 3 que es utilizado en CMM
- Las evaluaciones que son hechas con PAM tendrán resultados "más bajos"
- Las evaluaciones con PAM están basadas en atributos mucho más definidos y defendibles

Nivel de madurez Procesos COBIT 4.1	**Procesos con ISO/IEC 15504**	
	Nivel de capacidad	**Atributo**
5 Optimizado	5 Optimización	PA 5.1 innovación de proceso PA 5.2 optimización de proceso
4 gestionado y medible	4 Previsible	PA 4.1 medición de proceso PA 4.2 control de proceso
3 Definido	3 Establecido	PA 3.1 Definición de proceso PA 3.2 Despliegue de proceso
2 Repetible pero intuitivo	2 Gestionado	PA 2.1 Gestión de rendimiento PA 2.2 Gestión del trabajo del producto
1 Inicial/ ad hoc	1 Realizado	PA 1.1 Rendimiento del proceso
0 No existente	0 Incompleto	

Figura 11. Comparación de las escalas de capacidades utilizadas en Cobit 4.1 y PAM

El modelo de evaluación de procesos COBIT 4.1 utiliza un enfoque de evaluación de la capacidad definido en la norma ISO / IEC 15504. El objetivo es proporcionar una evaluación rigurosa, objetiva y repetible. Hay nueve atributos de madurez en la norma ISO 15504 y no son ni idénticos ni hay una relación directa entre ellos; los atributos de la ISO son por nivel de capacidad:

• PA5.1 Innovación de Procesos

• PA5.2 Optimización de Procesos

• PA4.1 Medición de Procesos

• PA4.2 Control de Procesos

• PA3.1 Definición del Proceso

• PA3.2 Implementación del Proceso

• PA2.1 Gestión del desempeño

[2] Modelo de Madurez de Capacidades o CMM (Capability Maturity Model) que fue desarrollado inicialmente para los procesos relativos al desarrollo e implementación de software por la Universidad Carnegie-Mellon para el SEI (Software Engineering Institute).

• PA2.2 Gestión del producto de trabajo

• PA1.1 Rendimiento de los procesos

El resultado clave de estas diferencias es que los resultados de la evaluación (en términos de niveles) pueden ser diferentes debido a que el modelo de evaluación del proceso de COBIT 4.1 (PAM) tiene criterios más precisos que el modelo de madurez de COBIT 4.1. Si bien es posible que los procesos sean calificados en el mismo nivel en los dos enfoques, la probabilidad es que los procesos obtendrán una calificación más baja en virtud de una evaluación realizada en contra del modelo de evaluación de procesos COBIT 4.1 (PAM).

Términos Y Definiciones

Para los efectos de este documento, se aplican los términos y definiciones dados en la Norma ISO / IEC 15504-1. Definiciones clave incluyen:

• Indicador de Atributo-Un indicador de evaluación que apoye el juicio de la medida del logro de un atributo de proceso específico (ISO / IEC 15504: 1, 3.16)

• Práctica Base -Una actividad que, cuando se realiza constantemente, contribuye al logro del propósito de un proceso específico (ISO / IEC 15504: 1, 3.17)

• Indicador de Capacidad-Un indicador de evaluación que apoye el juicio de la capacidad de proceso de un proceso específico (ISO / IEC 15504: 1, 3.19)

• Dimensión Capacidad-El conjunto de elementos en un modelo de evaluación de proceso relacionado explícitamente al marco de medición de la capacidad del proceso (ISO / IEC 15504: 1, 3.18)

• Práctica genérica-Una actividad que, cuando se lleva a cabo constantemente, contribuye al logro de un atributo de un proceso específico (ISO / IEC 15504: 1, 3.22)

• Indicador de rendimiento-Un indicador de evaluación que apoye el juicio del rendimiento de los procesos de un proceso específico (ISO / IEC 15504: 1, 3.26)

Nota: Un indicador de rendimiento es un indicador de atributo para el Atributo de Proceso 1.1 ara un proceso específico. (ISO / IEC 15504: 2)

• Modelo de evaluación de Proceso – un modelo adecuado para el propósito de evaluar la capacidad del proceso, basado en uno o más modelos de referencia de proceso (ISO / IEC 15504: 1, 3.33)

• Atributo de Proceso -una característica mensurable de la capacidad de proceso aplicable a cualquier proceso (ISO / IEC 15504: 1, 3.31)

• Clasificación del atributo de Proceso –Un juicio del grado de consecución del atributo de proceso para el proceso evaluado (ISO / IEC 15504: 1, 3.32)

• Capacidad de Proceso -Una caracterización de la capacidad de un proceso para cumplir con los objetivos del negocio actuales o proyectados (ISO / IEC 15504: 1, 3.33)

• Nivel de capacidad de proceso –un punto en la escala ordinal de seis puntos (de la capacidad del proceso) que representa la capacidad del proceso, cada nivel es construido sobre la capacidad del nivel inferior (ISO / IEC 15504: 1, 3,36)

• Clasificación del nivel de Capacidad de Proceso –Una representación del nivel de capacidad de proceso alcanzado derivado de la calificación del atributo del proceso para un proceso evaluado (ISO / IEC 15504: 1, 3.37)

• Resultado del Proceso -Un resultado observable de un proceso (ISO / IEC 15504: 1, 3.44)

Nota: Un resultado es un artefacto, un cambio significativo del estado o la reunión de las limitaciones especificadas.

• El propósito del proceso -El alto nivel de objetivos medibles de realizar el proceso y los posibles resultados de la aplicación efectiva del proceso (ISO / IEC 15504: 1, 3.47)

• Modelo de referencia del proceso –un modelo compuesto de definiciones de procesos en un ciclo de vida descrito en términos de propósito del proceso y los resultados, junto con una arquitectura que describe las relaciones entre los procesos (ISO / IEC 15504: 1, 3,48)

• Producto de trabajo -Un artefacto asociado a la ejecución de un proceso (ISO / IEC 15504: 1,3.55)

Descripción de la Arquitectura

El modelo de evaluación de procesos es un modelo bidimensional de la capacidad del proceso, como se muestra en la figura 12. En una dimensión, la dimensión de proceso, los procesos se definen y clasifican en categorías de proceso. En la otra dimensión, la dimensión de capacidad, un conjunto de atributos del proceso agrupados en niveles de capacidad definidos. Los atributos de proceso proporcionan las características de medición de la capacidad del proceso.

El modelo de evaluación de procesos se ajusta a los requisitos de la norma ISO / IEC 15504-2 para un modelo de evaluación de procesos, y se puede utilizar como la base para la realización de una evaluación de la capacidad de cada proceso de COBIT 4.1.

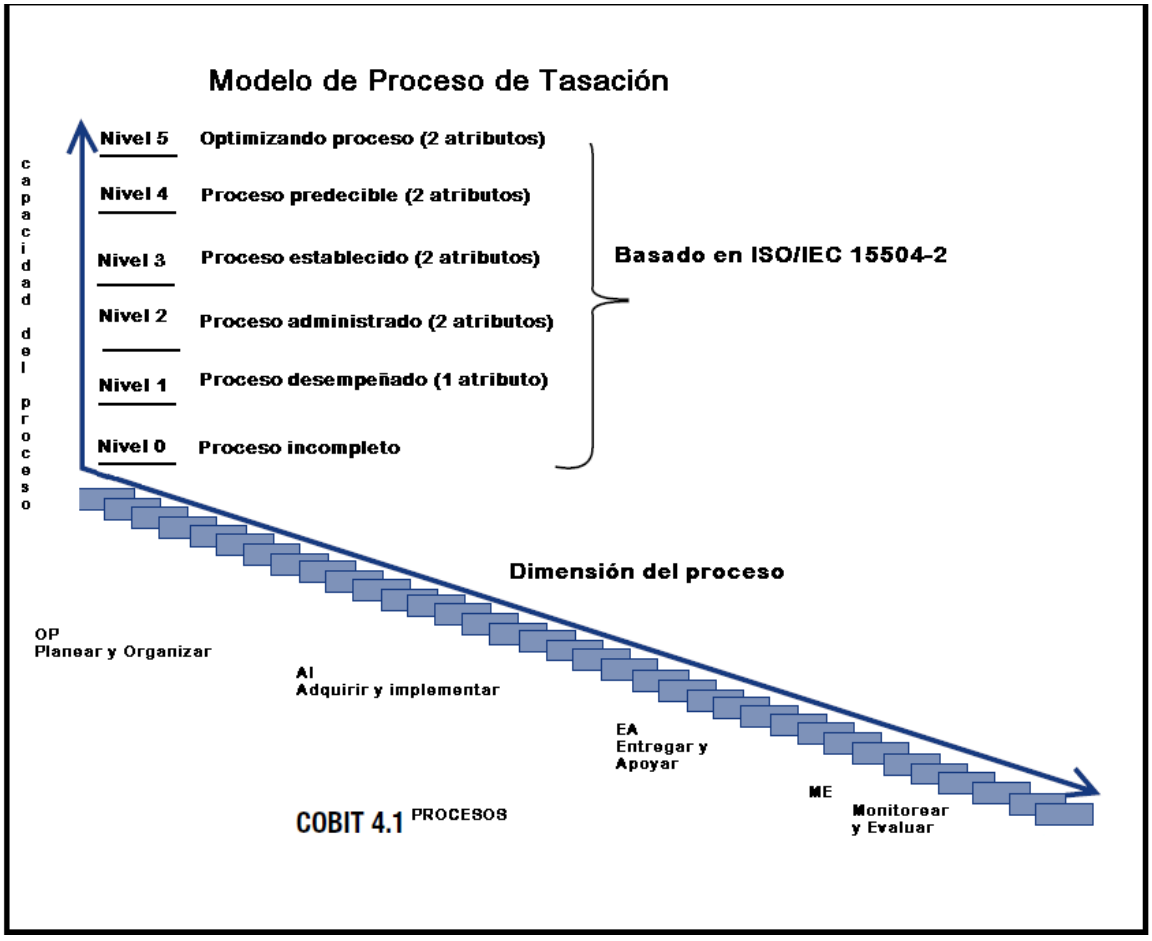


Figura 12. Vista general del modelo de evaluación de procesos (PAM)

La Dimensión de Procesos- Procesos COBIT 4.1

La dimensión de procesos utiliza COBIT 4.1 como el modelo de referencia de procesos. COBIT 4.1 proporciona definiciones de procesos en un ciclo de vida (el modelo de referencia de proceso), junto con una arquitectura que describe las relaciones entre los procesos.

El marco COBIT 4.1 se compone de 34 procesos que describen un ciclo de vida para la gobernanza de TI, como se muestra en la figura 13.

COBIT4.1 identifica los requisitos de los procesos de TI para el gobierno y la gestión de TI dentro de cuatro dominios. Los dominios se asignan a las áreas de responsabilidad tradicional de TI, planificación, construcción, ejecución y monitoreo. Estos dominios son:

Planificar y Organizar (PO): proporciona dirección a la entrega de soluciones (AI) y la prestación de servicios (DS) .Este ámbito abarca la estrategia y tácticas, se refiere a la identificación de la mejor forma en que TI puede contribuir a la consecución de los objetivos del negocio. La realización de la visión estratégica debe ser planificada, comunicada y administrada desde diferentes perspectivas. Una organización adecuada, así como la infraestructura tecnológica, se debe poner en su lugar.

Adquirir e Implementar (AI): proporciona las soluciones y las pasa a convertirse en servicios. Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas en el proceso de negocio. Los cambios en/y mantenimiento de los sistemas existentes también están cubiertos por este dominio, para asegurar que las soluciones sigan cumpliendo los objetivos de negocio.

Entregar y dar soporte (DS): Recibe las soluciones y las hace utilizables para los usuarios finales. Este dominio se refiere a la real prestación de los servicios requeridos, que incluye la prestación de servicios, la gestión de la seguridad y continuidad, apoyo de servicio para los usuarios, y gestión de datos e instalaciones operativas.

Monitorear y evaluar (ME): monitorea todos los procesos para asegurar que la dirección proporcionada se siguió. Todos los procesos de TI necesitan evaluarse regularmente con el tiempo por su calidad y el cumplimiento de los requisitos de control. Este dominio se dirige a la gestión del rendimiento, seguimiento del control interno, cumplimiento normativo y la gobernanza.

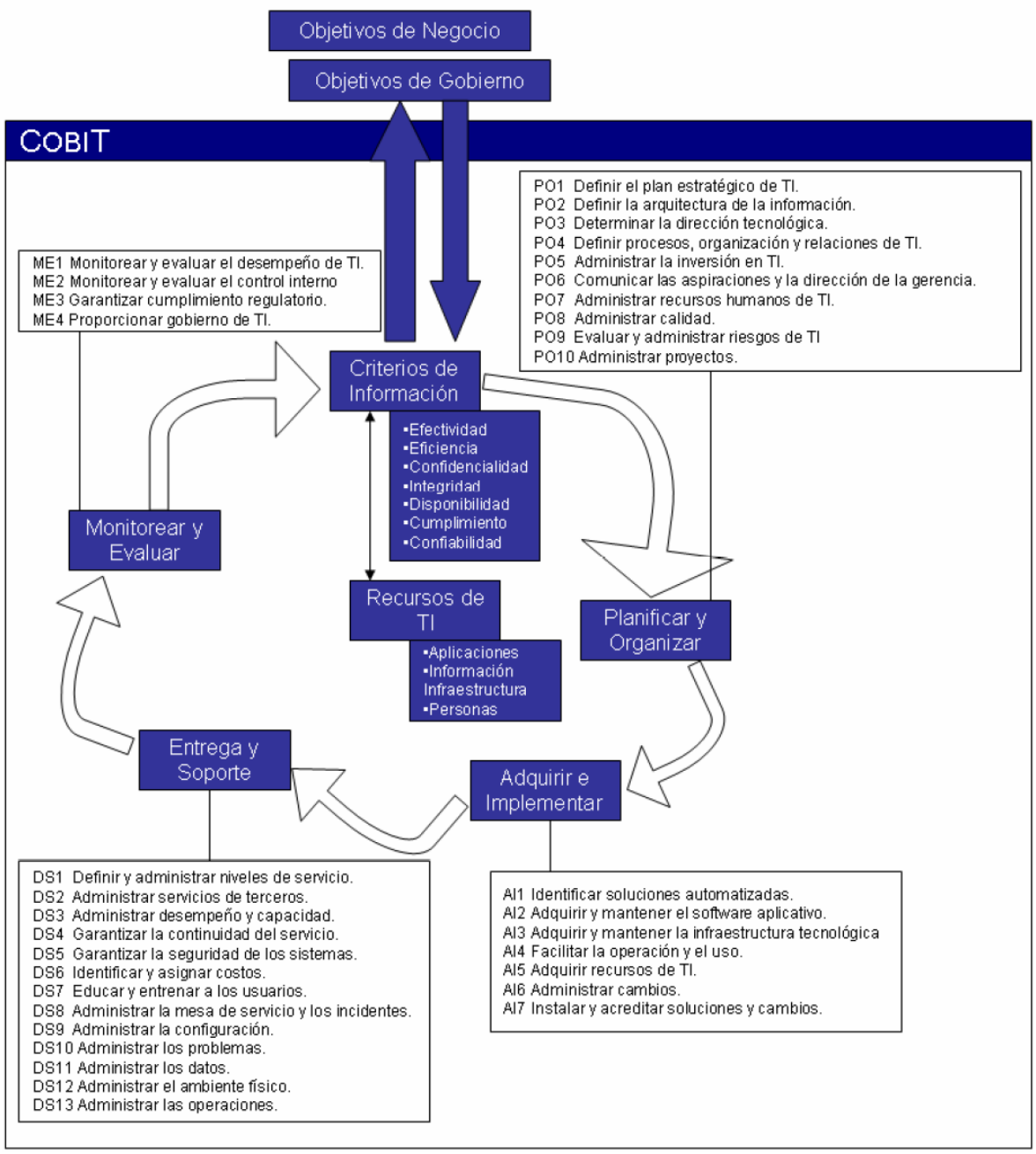


Figura 13. Marco Cobit 4.1

A través de los cuatro dominios hay 34 procesos de TI definidos. Los procesos de Cobit 4.1 son los siguientes

PO1 Definir un plan estratégico de TI.

PO2 Definir la arquitectura de la información.

PO3 Determinar la dirección tecnológica.

PO4 Definir los procesos de TI, la organización y las relaciones.

PO5 Administrar la inversión en TI.

PO6 Comunicar las aspiraciones y la dirección de gestión.

PO7 Administrar los recursos humanos.

PO8 Gestionar la calidad.

PO9 evaluar y gestionar los riesgos de TI.

PO10 Administrar proyectos.

AI1 Identificar soluciones automatizadas.

AI2 Adquirir y mantener software de aplicación.

AI3 Adquirir y mantener infraestructura tecnológica.

AI4 Habilitar operación y uso.

AI5 Procurar los recursos de TI.

AI6 Administrar cambios.

AI7 Instalar y acreditar soluciones y cambios.

DS1 Definir y gestionar los niveles de servicio.

DS2 Administrar los servicios de terceros.

DS3 Administrar el rendimiento y la capacidad.

DS4 Garantizar la continuidad del servicio.

DS5 Garantizar la seguridad de los sistemas.

DS6 Identificar y asignar costos.

DS7 Educar y entrenar a los usuarios.

DS8 Administrar la mesa de servicio y los incidentes.

DS9 Administrar la configuración.

DS10 Administrar los problemas.

DS11 Administrar los datos.

DS12 Administrar el ambiente físico.

DS13 Administrar las operaciones.

ME1 Monitorear y evaluar el desempeño de TI.

ME2 Monitorear y evaluar el control interno.

ME3 Garantizar el cumplimiento de los requisitos externos.

ME4 Proporcionar Gobierno de TI.

La Dimensión de Capacidad

La dimensión de capacidad proporciona una medida de la capacidad de un proceso para cumplir con los objetivos del negocio actuales o proyectados de una organización para el proceso.

La capacidad del proceso se expresa en términos de atributos de proceso agrupados en niveles de capacidad, como se muestra en la figura 14. El nivel de capacidad de un proceso se determina sobre la base de la consecución de los atributos de un proceso específico según la norma ISO / IEC 15504-2: 2003.

La escala de evaluación consta de seis niveles de capacidad de la siguiente manera:

Nivel 0 Proceso Incompleto. El proceso no se ha implementado o fallo para lograr el propósito del proceso. En este nivel, hay poca o ninguna evidencia de cualquier logro sistemático del propósito del proceso.

Nivel 1 Proceso ejecutado (un atributo). El proceso implementado logra el propósito del proceso.

Nivel 2 proceso administrado (dos atributos). El proceso realizado descrito previamente ahora se implementa de una manera administrada (planificada, controlada y ajustada) y su productos de trabajo se establecen, controlan y mantienen apropiadamente.

Nivel 3 proceso establecido (dos atributos). El proceso administrado descrito previamente ahora se implementa utilizando un proceso definido que es capaz de alcanzar los resultados del proceso.

Nivel 4 proceso predecible (dos atributos). El proceso establecido previamente descrito ahora opera dentro de los límites definidos para lograr sus resultados del proceso.

Nivel 5 proceso de Optimización (dos atributos). El proceso predecible descrito anteriormente es continuamente mejorado para cumplir con los objetivos relevantes actuales y proyectados del negocio.

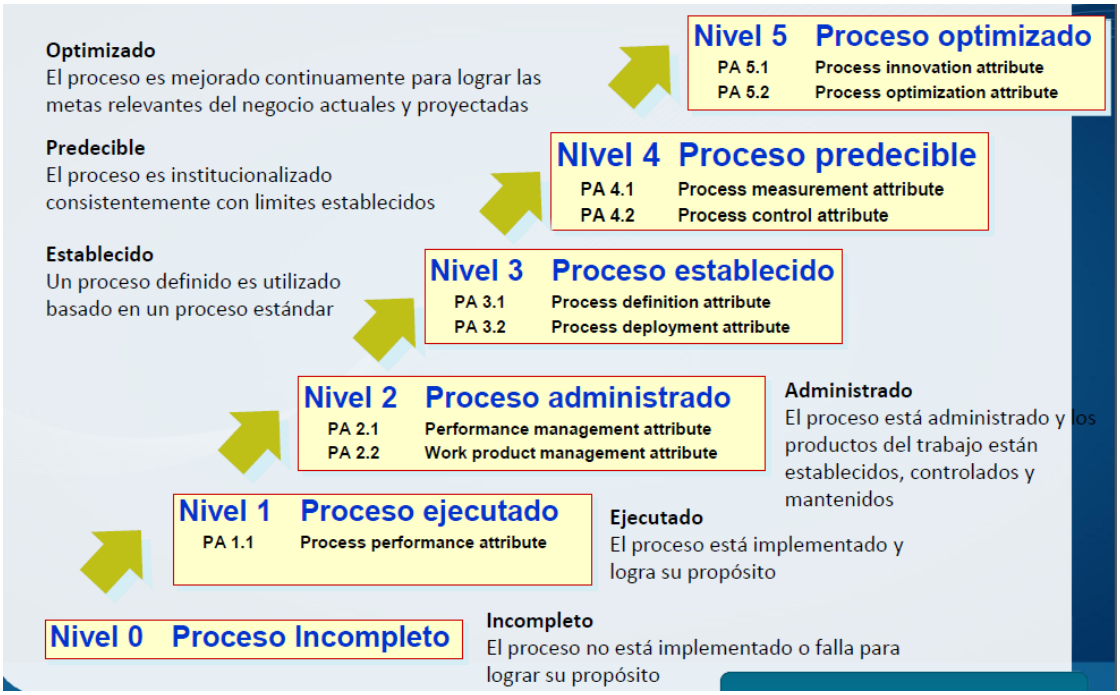


Figura 14. Niveles de Capacidad y Atributos de Procesos

Indicadores de Evaluación

Indicadores de evaluación se utilizan para evaluar si atributos de proceso se han logrado (ver Figura 15).

Hay dos tipos de indicadores de evaluación:

• Indicadores de capacidad de los procesos, que se aplican a los niveles de capacidad de 1 a 5.

• Los indicadores de desempeño de los procesos, que se aplican exclusivamente al nivel de capacidad 1.

Indicadores de desempeño de procesos (prácticas base y productos de trabajo) son específicos para cada proceso y son utilizados para determinar si un proceso está en capacidad del

nivel 1. Las prácticas base y productos de trabajo para cada proceso se basan en el material de COBIT 4.1.

Los indicadores de capacidad de proceso son genéricos para cada atributo del proceso para los niveles de capacidad de 1 a 5.

Los indicadores de capacidad del proceso utilizados en COBIT 4.1 evaluación de la capacidad de proceso son:

• Práctica genérica (GP)

• Producto de trabajo genérico (GWP)

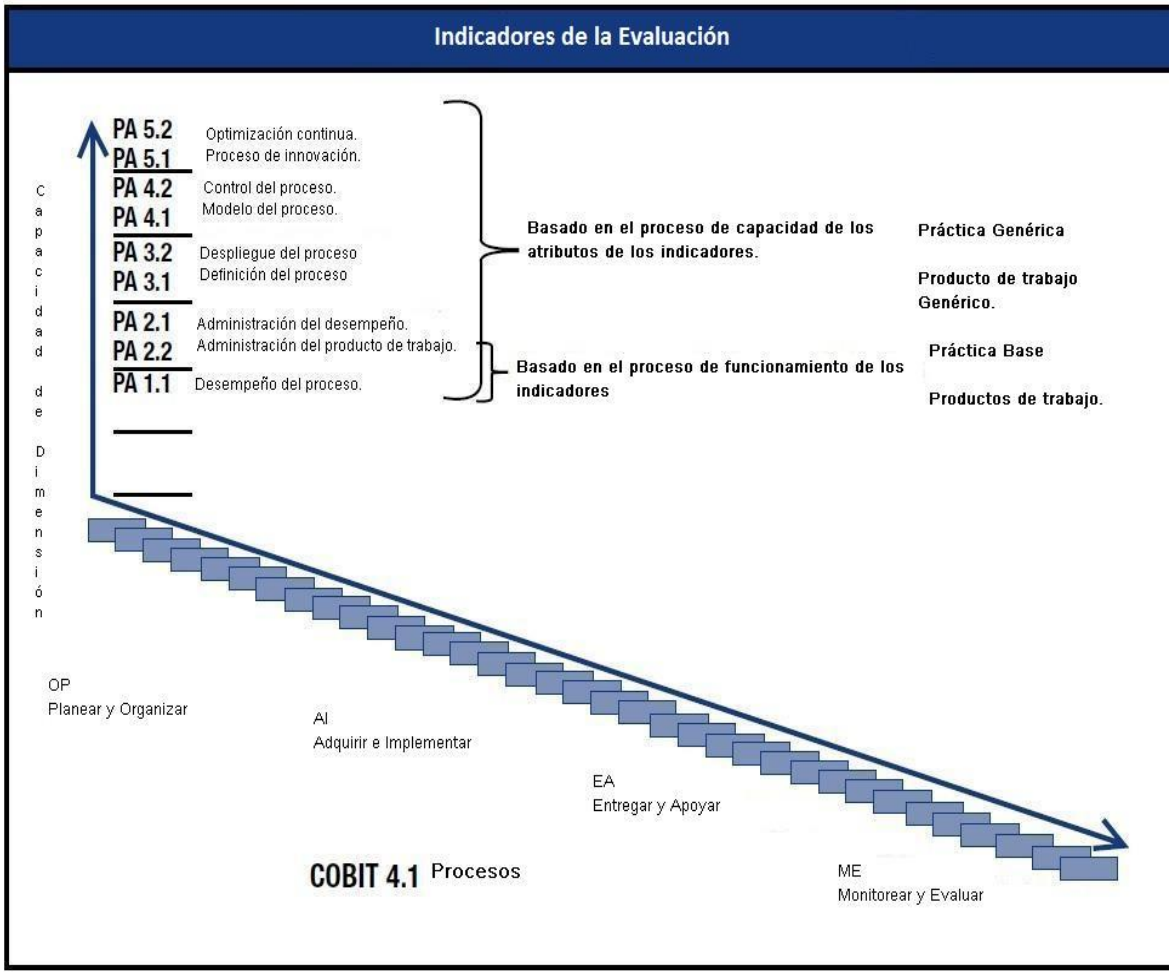


Figura 15. Indicadores de Evaluación

Dimensión del Proceso e Indicadores de Desempeño del Proceso

Los procesos en la dimensión de proceso se pueden asignar directamente a los procesos definidos en el modelo de referencia de proceso.

Los procesos individuales se describen en términos de nombre del proceso, propósito y resultados (Os), basado en COBIT 4.1.

Además, la dimensión de proceso del modelo de evaluación de proceso proporciona información en forma de:

• Un conjunto de prácticas base (BP) para el proceso, proporcionando una definición de las tareas y actividades necesarias para llevar a cabo el propósito del proceso y cumplir con los resultados del proceso. Cada BP se asocia explícitamente a un resultado del proceso.

• Un número de entrada y salida de productos de trabajo (WPS) asociados con cada proceso y relacionados con uno o más de sus resultados.

• Características asociados a cada WP

El BP y WPS constituyen el conjunto de indicadores de desempeño de los procesos. Los WPs asociados que se listan pueden utilizarse para la revisión de las entradas y salidas potenciales de la implementación de procesos de una organización.

Los WPs asociados brindan orientación objetiva para las entradas y salidas potenciales para buscar y sustentar evidencia objetiva a la evaluación de un proceso en particular. Es necesario documentar el proceso de evaluación y el juicio del evaluador para asegurar que el contexto de proceso (dominio de aplicación, el objetivo comercial, metodología de desarrollo, el tamaño de la organización, etc.) se considera explícitamente al utilizar esta información.

Esta lista de WPs no debe considerarse un checklist de lo que cada organización debe tener, sino más bien como un ejemplo y punto de partida para considerar si, dado el contexto, los WP son necesarios y contribuyen a la finalidad prevista del proceso.

Cabe señalar que los WPS para algunos procesos proporcionan los requisitos de capacidad más altos para otros procesos. Esto resultará en una implementación progresiva de los procesos. El enfoque inicial en cualquier evaluación de procesos serían los procesos centrales (a veces llamados procesos primarios) que son principalmente parte de los dominios de IA y DS. Procesos en los dominios PO y ME serán requeridos para mejorar el apoyo en la capacidad de éstos procesos centrales más allá del nivel 1.

Indicadores de Capacidad de Proceso

Indicadores de capacidad de proceso son los medios para alcanzar las capacidades abordados por los atributos de proceso. Evidencia de los indicadores de capacidad de proceso apoyan el criterio del grado de consecución de la PA.

El modelo de evaluación de procesos describe los indicadores de capacidad de procesos relacionados con los atributos de proceso (AP) asociados con los niveles de capacidad de 1 a 5 definido en la dimensión de capacidad del modelo de evaluación de proceso.

La dimensión de capacidad del modelo de evaluación de proceso consta de seis niveles de capacidad que coinciden con los niveles de capacidad del modelo de evaluación de proceso.

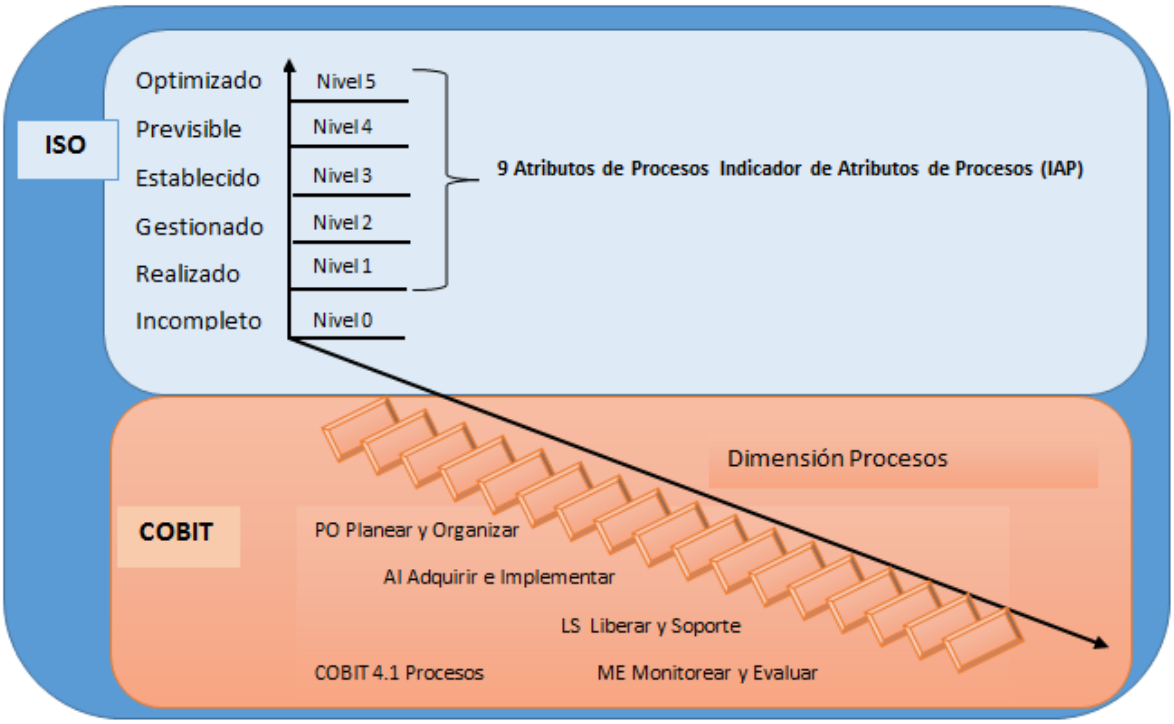
Marco para la Medición

El proceso de evaluación de COBIT mide la extensión en la cual un proceso dado logra los atributos específicos relativos a ese proceso – "atributos del proceso"

•El proceso de evaluación de COBIT define 9 atributos de los procesos (basados en ISO/IEC 15504-2)

- –PA 1.1 Rendimiento de los procesos
- –PA 2.1 Gestión del rendimiento
- –PA 2.2 Gestión de productos de trabajo
- –PA 3.1 Definición de proceso
- –PA 3.2 Despliegue de procesos
- –PA 4.1 Medición de proceso
- –PA 4.2 Control de proceso
- –PA 5.1 Innovación de procesos
- –PA 5.2 Optimización continua

Atributos de Procesos y Niveles de Capacidad (Ver figura 16)



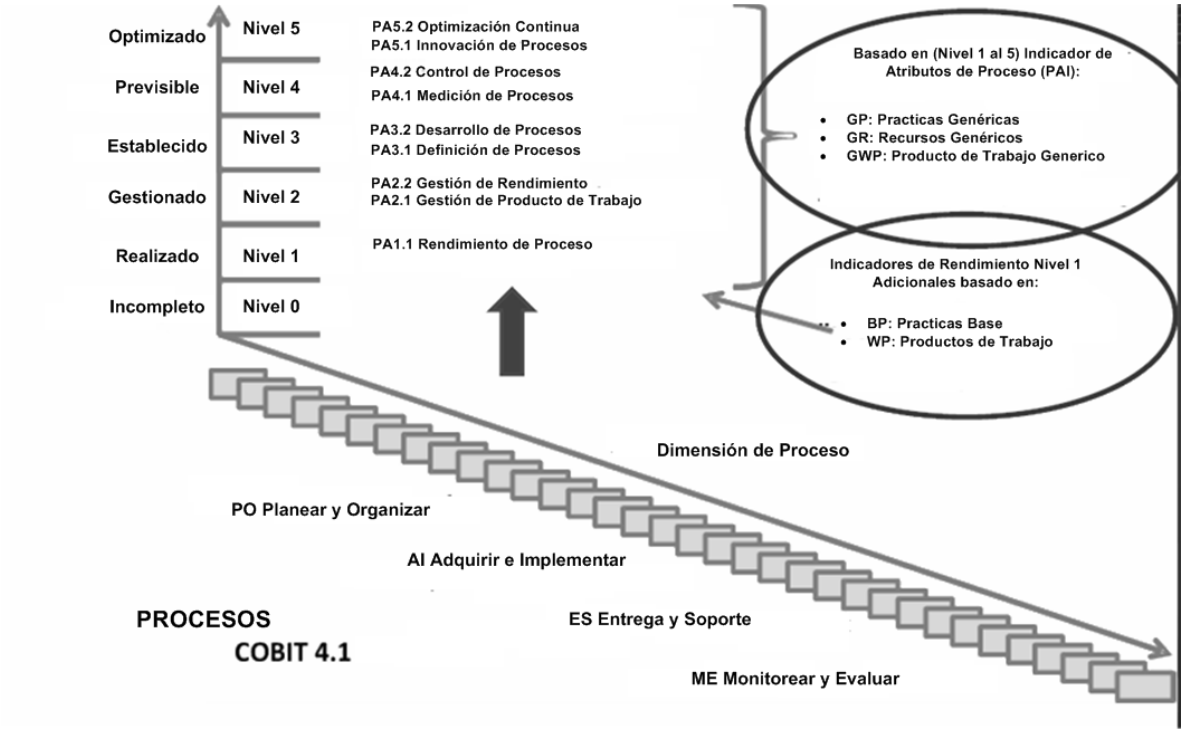


Figura 16. Atributos de Procesos y Niveles de Capacidad

- Los indicadores de la evaluación en el PAM son utilizados para soportar el juicio de los asesores en la clasificación de los atributos de los procesos:
  - Proveen la base para la repetitividad en las evaluaciones
- La clasificación se asigna basada en una evidencia objetiva y validada para cada atributo del proceso.
- Debe mantenerse la trazabilidad entre la clasificación de un atributo y la evidencia objetiva utilizada para determinar esa clasificación.

2.3.4 Information Security Management Maturity Model ISM3 (Aceituno, 2011)

Antecedentes

El punto de inicio de ISM3 fue tomar las mejores ideas acerca de los sistemas de gestión y controles como ISO 9000, ITIL, CMMI y ISO 17799/ ISO 27001.

ISM3 nació con la intención de ayudar tanto a las grandes organizaciones como a las pequeñas a obtener el máximo retorno de su inversión en seguridad, sea cual sea su presupuesto, a menudo en relación con el uso de un SGSI.

Introducción

El Modelo de Madurez Abierto de Gestión de la Seguridad de la Información (del inglés, Open Information Security Managment Maturity Model / O-ISM3) es el marco de trabajo (framework) para manejar la seguridad de la información del Open Group.

El Open Group es un consorcio neutral de tecnología y de fabricantes de la industria, el cual habilita el acceso a información integrada dentro y entre la empresa, basada en estándares abiertos e interoperabilidad global. El Open Group trabaja con clientes, proveedores, consorcios y cuerpos de otros estándares. El consorcio cuenta con 15 años de experiencia en desarrollar y operar programas de certificación.

ISM3 define un comprensible pero manejable número procesos de seguridad de la información para las necesidades de la mayoría de las organizaciones, con la identificación de controles de seguridad relevantes dentro de cada proceso, concibiéndose como un subconjunto de esos procesos. En este sentido es completamente compatible en este campo de la seguridad de la información con los estándares ISO/IEC 27000:2009, COBIT e ITIL.

ISM3 provee un marco de trabajo para construir, confeccionar y operar un SGSI. ISM3 define madurez en términos de la operación de procesos de seguridad claves y Capacidad es definida en términos de las métricas y prácticas de gestión utilizadas.

Las organizaciones de diferentes sectores de negocio y países tienen diferentes requerimientos del negocio y tolerancias de riesgo. ISM3 apoya a los Administradores de la Seguridad de la Información a evaluar su propio ambiente operativo y planificar sus procesos de gestión de la seguridad, de manera que pueden ser consistentes y efectivos financieramente con los objetivos del negocio.

Alcances

ISM3 puede utilizarse como una herramienta de evaluación y mejora para auditores y administradores del Sistema de Gestión de Seguridad de la Información, puede ser utilizada para extender las disciplinas de las ISO 9000 dentro un SGSI, posee la capacidad de ser utilizado para certificar un SGSI o es un estándar certificable y tiene compatibilidad con ISO/IEC27000, ITIL, ISO 9000 y COBIT.

Objetivos

- Reducir la brecha entre la capacidad SGSI según se define en ISO 27001, el catálogo de los controles de las mejores prácticas identificadas en ISO27002 y la necesidad de que el personal de gestión de seguridad de la información tienen para mejorar continuamente su gestión de la seguridad interna utilizando métricas y modelos de madurez.
- Permitir a las organizaciones a identificar y alcanzar los niveles de gestión de seguridad de información adecuada a su industria, perfil de riesgo y a su tamaño.
- Proporcionar a las organizaciones oportunidades de certificación, de manera que las organizaciones que han certificado su programa de gestión de seguridad de la información a un nivel dado de ISM3 pueden ser reconocidos por su programa de madurez y por lo tanto

pueden proporcionar un cierto nivel de fiabilidad independiente a sus clientes en cuanto a la rigurosidad con la que se trata la seguridad de la información.

- Proporcionar las bases para un ecosistema de la industria para desarrollar todo el área de gestión de seguridad de la información, incluso para formadores en metodología ISM3, la certificación de las implementaciones y profesionales ISM3 y posiblemente, para los proveedores de software de información y herramientas de gestión de la seguridad.

Características Clave

- Basada en un enfoque completamente en procesos de gestión de la seguridad de la información y madurez, sobre el principio que cada control necesita un proceso para ser manejado.
- Rompe la gestión de la seguridad de la información en un amplio pero manejable número de procesos, con controles de seguridad específicamente relevantes a ser identificados dentro de cada proceso como un subconjunto principal de ese proceso.
- Define la madurez de la gestión de la seguridad de la información en términos de la operación de un adecuado y complementario conjunto procesos de seguridad de información ISM3.
- Define la Capacidad en términos de métricas y las prácticas de gestión utilizadas.
- Los Niveles de Madurez ayudan a las organizaciones a seleccionar la escala SGSI más apropiada para sus necesidades.
- El espectro de la madurez facilita el equilibrio de costos, riesgo, la usabilidad y habilita la mejora incremental, benchmarking y objetivos a largo plazo.
- Ofrece un enfoque a las organizaciones de flexibilidad para seleccionar cualquier subconjunto de procesos de seguridad de la información basado en criterios variados.

Ventajas o Beneficios

Amigable con el negocio

ISM3 es un estándar que no tiene por objeto la invulnerabilidad o la seguridad absoluta. ISM3 alinea la gestión de seguridad con las necesidades del negocio a través Objetivos del Negocio, Objetivos de Seguridad y Metas de Seguridad. Objetivos de Seguridad y las Metas de Seguridad ayudan a la alta dirección y las partes interesadas a claramente ver y comprender el vínculo entre el negocio y la seguridad de la información. Esta orientación hace al ISM3 aplicable a todas las clases de organizaciones: Pequeñas, grandes, privadas, públicas y de caridad.

Adaptable

ISM3 tiene 5 niveles de madurez, cada uno puede ser acreditado como un sistema de gestión. Usando estos niveles, una organización puede adaptar su SGSI a Metas de Seguridad reales, utilizando los recursos a fin de maximizar la mejora.

Otra ventaja de los niveles de madurez, es que es posible obtener certificaciones intermedias cuando se alcanzan ciertas metas en camino de alcanzar niveles más altos del SGSI.

Los niveles de madurez pueden simplificar el diseño del SGSI, desde un cierto nivel se puede encontrar uno adecuado para las necesidades de toda la organización.

Acreditable

Un SGSI basado en ISM3 es acreditable bajo la norma ISO 9001 o ISO/IEC 27001, lo cual quiere decir que se puede usar ISM3 para implementar SGSI basado en ISO 27001. La definición de procesos ISM3 se derivan de CMMI e ISO 9001. Esto significa que un sistema ISM3 puede ser acreditado cuando un auditor encuentra evidencia de que todos los procesos pertenecen a cierto nivel de madurez.

Fácil de Implementar

Existe una clara división de responsabilidades entre líderes, administradores y personal técnico usando los conceptos de Gestión Estratégica, Táctica y Operacional.

Es fácil determinar responsabilidades de seguridad gracias a la división de los procesos ISM3 en capas o niveles.

Niveles de Gestión
Estratégico – Directa y Provee
Táctico – Implementa y Optimiza
Operacional – Ejecuta y Reporta

Implementación de SGSI basado en ISM3

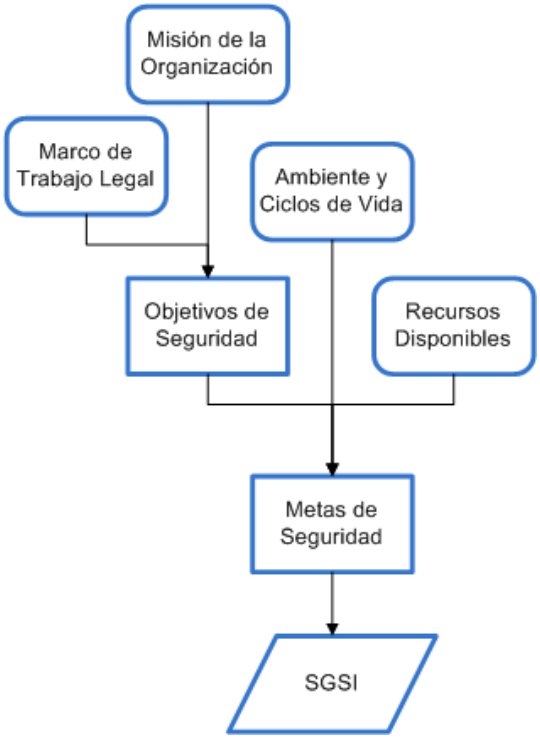


Figura 17. Implementación d SGSI basado en ISM3

Compatible (Ver Figura 17)

ISM3 es compatible con ISO 27001 en el punto que ISM3 puede ser utilizada como una herramienta que ayuda a la implementación de ISO 27001 o incluso para certificar una organización con los dos estándares. También es compatible con ITIL y COBIT.

Escalable y Completa

ISM3 reconoce la existencia de diferentes ambientes dentro de una organización, como roles, necesidades de protección, ambiente de producción, desarrollo, etc. Es escalable desde pequeñas organizaciones hasta conglomerados internacionales.

Utilizar ISM3 fomenta la colaboración entre clientes y proveedores de seguridad de la información.

ISM3 trata a ambas amenazas tanto técnicas como no técnicas, como el fraude, la corrupción y los errores humanos mediante el uso de la transparencia, el particionamiento, la supervisión, la rotación y la separación de responsabilidades.

Abierto

ISM3 está publicado bajo licencia de Creative Commons y su versión electrónica esta libremente disponible.

Basada en procesos

ISM3 utiliza un enfoque orientado a procesos hacia una Gestión de Seguridad de la Información. ISM3 define la Seguridad de la Información como resultado de un conjunto de procesos.

La definición de un proceso incluye varios componentes, tales como el dueño de proceso, el alcance de la protección, las actualizaciones en el control, la disponibilidad de sistemas protegidos por el proceso, etc.

Uso de Métricas

ISM3 hace seguridad de la información un proceso medible a través del uso de métricas para cada proceso. El principio seguido es. “Lo que no se puede medir, no se puede gestionar y lo que no se gestiona, no se puede mejorar”

Los procesos de seguridad de la información son manejables a través de métricas. Esto permite a los administradores mostrar resultados, muestran cómo los resultados benefician a la organización, y comprobar qué los ajustes en el proceso, hacen que el proceso se mejore. También facilita la rendición de cuentas.

Descripción de Estándar ISM3

Definición de términos clave

- **Proceso:** El proceso es la unidad más pequeña y atómica del estándar. ISM3 se centra alrededor del concepto de proceso. Los procesos tienen capacidades y se administran mediantes prácticas de gestión.

- **Capacidad:** Las métricas del proceso habilitan sus prácticas de gestión y revelan su capacidad. Desde el punto de vista de un auditor, las métricas del proceso determinan su capacidad.
- **Madurez:** Los procesos ISM3 seleccionados que se recogen juntos y operan con una capacidad suficiente determina la madurez de la gestión de la seguridad de la información de una organización o simplemente su madurez. Los niveles de madurez y capacidad pueden ser usados como base para el desarrollo de un esquema de certificación, lo que puede ser de especial valor para las autoridades certificadoras (auditores).

Vinculando los tres términos juntos

La siguiente tabla especifica que métricas se necesitan para que un proceso alcance cada nivel de capacidad y su respectiva asignación de las prácticas de gestión.

Las métricas habilitan la capacidad de moverse desde un estado base a un estado óptimo.

La capacidad del proceso está determinada por las métricas que el proceso produce. Las métricas son clasificadas por tipo. Hay cinco niveles de capacidad de proceso: básico, definidos, gestionados, controlados y optimizados. Las métricas se clasifican en siete tipos posibles (ver tabla 11).

Nivel de Capacidad	**Inicial**	**Gestionado**	**Definido**			**Controlado**	**Optimizado**
Prácticas de Gestión habilitadas	**Auditar, Certificar**	**Prueba**	**Monitoreo**	**Planificación**	**Beneficios de Realización**	**Evaluación**	**Optimización**
Documentación		*	*	*	*	*	*
Tipo de Métrica	Actividad		*	*	*	*	*
	Alcance		*	*	*	*	*
	Indisponibilidad		*	*	*	*	*
	Efectividad		*	*	*	*	*
	Carga			*	*	*	*
	Calidad					*	*
	Eficiencia						*

Tabla 11. Niveles de Capacidad de Proceso

Niveles de Capacidad

Ampliando la definición, *capacidad* es una propiedad de como un proceso es gestionado. Desde una perspectiva de gestión, a mayor la capacidad, mayor las prácticas de gestión que sean de aplicación, mayor robustez, transparencia y autocorrección de procesos. Desde la perspectiva del auditor, la capacidad alcanzada por un proceso depende de la documentación y métricas utilizadas para su gestión.

Algunos factores que ayudan a alcanzar mayores niveles de capacidad son una apropiada distribución de responsabilidades, los recursos disponibles para el proceso y la motivación, habilidades, responsabilidad y empoderamiento del personal.

Niveles de Madurez

Los niveles de madurez ISM3 son combinaciones específicas de procesos ISM3 practicados en los niveles de capacidad especificados. Los procesos se asignan a los niveles de madurez certificables según el espectro, desde un ISM3 básico a uno avanzado. Hay una relación entre el número de procesos, su capacidad y la madurez del SGSI. A más procesos y cuanto mayor sea la capacidad, mayor es la madurez. Las relaciones clave detrás de los niveles de madurez de ISM3 son:

- Mapeo (o agrupación) de los procesos para cada nivel de madurez ISM3
- Definir la capacidad de cada proceso mapeado a cada nivel de madurez ISM3

Los niveles de madurez están diseñados para satisfacer las necesidades de organizaciones con diferentes:

- Tamaños
- Recursos
- Amenazas
- Impacto (económico y reputación)
- Apetito de Riesgo
- Sector económico

Tipos de organizaciones incluyendo pequeñas, medianas, grandes, de gobierno, subcontratistas de procesos de negocio, especialistas en comercio electrónico, organizaciones de infraestructura critica, proveedores de servicios de software y servicios en la nube y proveedores de seguridad.

Procesos

ISM3 identifica cuatro niveles de gestión de seguridad (ver tabla 12) sobre la base que cada nivel de proceso reporta al superior, de esa manera únicamente el Nivel Estratégico reporta al Director Ejecutivo.

Niveles de Gestión
Estratégico – Directa y Provee • Coordinar • Objetivos de Seguridad – Política de Seguridad • Provee recursos
Táctico – Implementa y Optimiza • Diseña el Sistema de Gestión de Seguridad de la Información (SGSI) • Gestiona Recursos
Operacional – Ejecuta y Reporta • Alcanzar los objetivos definidos • Procedimientos técnicos

Tabla 12. Niveles de Gestión de Seguridad

ISM3 define un número de procesos, los cuales están agrupados en cuatro tipos de niveles (Ver tabla 13).

Niveles de Procesos
Procesos Genéricos (del inglés, Generic Processes (GP))
Procesos Estratégicos Específicos (del inglés, Strategic-Specific Processes (SSP))
Procesos Tácticos Específicos (del inglés, Tactical-Specific Processes (TSP))
Procesos Operativos Específicos (del inglés, Operational-Specific Processes (OSP))

Tabla 13. Niveles de Proceso

Procesos Genéricos

Los Procesos Genéricos proveen la infraestructura esencial para la implementación, evaluación y mejora de un proceso de SGSI. Que comprende:

- Gestión de Conocimiento
- Auditoria de SGSI y del Negocio
- Diseño/Evolución que define las relaciones con otras organizaciones
- Asigna recursos para la seguridad de la información
- Define objetivos de seguridad consistentes con los objetivos del negocio
- Define el esquema organizacional de delegación
- La Gestión de Seguridad de la Información (GSI)

Procesos Estratégicos Específicos

La gestión estratégica es responsable de seleccionar y diseñar servicios que proveen valor dentro los recursos económicos y paramentos de riesgo de la organización. La gestión estratégica le rinde cuentas a los grupos de interés (stakeholders) para el uso de los recursos a través de acuerdo de gobernabilidad.

La gestión estratégica cumple los siguientes objetivos específicos y responsabilidades con respecto a la seguridad.

- Provee liderazgo y coordinación de seguridad de la información, seguridad física, seguridad del lugar de trabajo e interacción con otras unidades organizacionales
- Revisa y Mejora el SGSI

Procesos Tácticos Específicos

La gestión estratégica es cliente de la gestión táctica con respecto a los procesos de Gestión de Seguridad de la Información (GSI). La gestión táctica rinde cuentas a la gestión estratégica para rendimiento del SGSI y del uso de recursos.

La gestión táctica tiene los siguientes objetivos específicos y responsabilidades:

- Provee retroalimentación a la gestión estratégica

- Gestiona el presupuesto, personas y otros recursos asignados a la seguridad de la información
- Define el ambiente para la gestión operacional:
    - Metas de Seguridad y Clasificación de Activos
    - Arquitectura de Seguridad y Ciclo de Vida de Gestión
    - Acuerdo de Nivel de Gestión
    - Gestión de Seguros
    - Personal de Seguridad
    - Información de Operaciones

Procesos Operacionales Específicos

La gestión operacional reporta al Director de Información y al Gerente de Seguridad Táctica.

La gestión operacional tiene los siguientes objetivos específicos y responsabilidades:

- Provee retroalimentación a la gestión táctica, incluyendo reportes de incidentes y métricas
- Procura y aplica los recursos asignados de forma efectiva y eficiente
- Identifica y protege los activos dentro de los ciclos de vida
- Protege y da soporte a los sistemas de información en su ciclo de vida
- Aplica gestión de acceso y controles ambientales para los usuarios y servicios
- Gestiona la disponibilidad
- Testea y audita
- Monitorea y gestiona el ciclo de vida de las medidas de seguridad
- Efectúa procesos para prevenir incidentes, detectarlos y mitigarlos.

Procesos ISM3

Procesos Genéricos
GP-1: Gestión del Conocimiento
GP-2: SGSI y Auditoria del Negocio
Implementando ISM3
GP-3: Diseño de GSI y Evolución

Procesos Específicos – Gestión Estratégica
SSP-1: Reportar a los grupos de interés
SSP-2: Coordinación
SSP-4: Define las reglas de la división de funciones
SSP-6: Asignar Recursos para la Seguridad de la Información

Procesos Específicos – Gestión Táctica
TSP-1: Reportar a Gestión Estratégica
TSP-2: Administrar los Recursos Asignados
TSP-3: Definir Metas de Seguridad y Objetivos de Seguridad
TSP-4: Gestión del Nivel de Servicio

TSP-6: Arquitectura de Seguridad
TSP-13: Gestión de Seguros
Seguridad de Personal
TSP-7: Revisión de Antecedentes
TSP-8: Seguridad de Personal
TSP-9: Formación de Personal de Seguridad
TSP-10: Proceso Disciplinario
TSP-11: Concientización de Seguridad
TSP-14: Operaciones de Información

Procesos Específicos – Gestión Operacional
OSP-1: Reportar a la Gestión Táctica
OSP-2: Adquisición de Seguridad
Control de Ciclo de Vida
OSP-3: Gestión de Inventario
OSP-4: Control de Cambios Gestionado por Sistemas de Información de TI
OSP-5: Aplicación de Parches Gestionados por TI
OSP-6: Compensación Gestionado por TI
OSP-7: Endurecimiento Gestionado por TI
OSP-8: Control de Ciclo de Vida de Desarrollo de Software
OSP-9: Medidas de Seguridad en Control de Cambios
OSP-16: Segmentación y Gestión de Filtrado
OSP-17: Gestión de Protección contra Malware
Control de Acceso y Ambiente
OSP-11: Control de Acceso
OSP-12: Registro de Usuario
OSP-14: Gestión para Protección de Ambiente Físico
Control de Disponibilidad
OSP-10: Gestión de Respaldos
OSP-15: Gestión de Continuidad de Operaciones
OSP-26: Confiabilidad Reforzada y Gestión de Disponibilidad
OSP-27: Gestión de Archivado
Pruebas y Auditoria
OSP-19: Auditorias Técnicas Internas
OSP-20: Emulación de Incidentes
OSP-21: Evaluación de Calidad de Información y Cumplimiento
Monitoreo
OSP-22: Monitoreo de Alertas
OSP-23: Detección y Análisis de Eventos Internos
OSP-28: Detección y Análisis de Eventos Externos
Manejo de Incidentes
OSP-24: Manejo de Incidentes y Potenciales Incidentes
OSP-25: Forense

Selecciona tu conjunto de Procesos

El conjunto de procesos que una organización debe seleccionar para ser usados en una implementación ISM3 depende de su Política de Seguridad, reconciliada con los recursos que están disponibles para invertir en controles de seguridad y operar la función de la gestión de seguridad.

Definición de Procesos

ISM3 define un conjunto comprensivo de procesos de gestión de seguridad de la información que son aplicables al manejo de la seguridad de la información. Los usuarios de ISM3 deben conocer que estos procesos representan un recurso de negociación entre los intereses del negocio.

La notación utilizada para los procesos ISM3 (ver tabla 14) describe ciertas propiedades:

Proceso	Código y Nombre de Proceso
Descripción	Resumen de la actividad ejecutada en el proceso
Valor	Explicación de los beneficios esperados del proceso
Documentación	Políticas, procedimientos y plantillas. Definición de procesos necesarios para describir y ejecutar el proceso
Entradas	Entradas al proceso
Salidas	Resultado de los procesos
Descripción de métricas	Definición de medidas apropiadas cubriendo exactitud, precisión y otras mediciones de calidad de salida según sea apropiado.
Responsabilidades	Dueños de procesos, Supervisor de procesos
Procesos Relacionados	Otros procesos ISM3 que requieren entradas a este proceso
Metodologías Relacionadas	Metodologías reconocidas y buenas prácticas. Las metodologías mencionadas deben ser útiles para planificar, evaluar, implementar, probar, monitorear, auditar, optimizar y certificar el proceso

Tabla 14. Notación utilizada para los procesos ISM3

Roles y Responsabilidades de Proceso

Para llevar una responsabilidad adecuada la persona o equipo debe ser:

- Tener un interés personal en el resultado
- Competente
- Motivado
- Empoderado

Reglas de división de funciones para transparencia, particionamiento, supervisión, rotación y separación de responsabilidades ayudan a prevenir conflictos de interés y colusiones (es un pacto para que acuerdan para perjudicar un tercero) para cometer y encubrir actividad no autorizada, incluyendo actividad potencialmente criminal.

Una apropiada distribución de responsabilidades, provisión de recursos y el uso de procesos ISM3 ayudan a mejorar el rendimiento del personal.

Describiendo la estructura organizacional, las siguientes definiciones son utilizadas:

Dueño de Procesos: La persona o el equipo responsable de ejecución del proceso.

Rol: Un conjunto de responsabilidades asignados a una persona o equipo.

Organigrama: Diagrama de las responsabilidades para supervisión entre roles.

Límites: Define los límites de la organización

Los siguientes roles tienen especial importancia en ISM3:

Cliente: Un cliente es el rol quien provee recursos y conjuntos de requerimientos para un proceso o un dueño de proceso.

Gestión Estratégica: Administradores involucrados en la alineación a largo plazo de TI con las necesidades del negocio.

Gestión Táctica: Administradores involucrados en la asignación de recursos y la configuración y gestión del SGSI.

Gestión Operacional: Administradores involucrados en el establecimiento, operación y monitoreo de procesos específicos.

Los roles definidos anteriormente reconocen que un individuo puede tener más de un rol como lo podría suceder en una pequeña organización.

Definición de Métricas de Procesos

Las métricas son utilizadas para promover mejoras que incrementan el valor agregado por un proceso. ISM3 se enfoca en las métricas que son relevantes a la gestión de procesos

ISM3 define los siguientes tipos de métricas (ver tabla 15):

Tipo de Métrica	Descripción
Actividad	Número de salidas producidas.
Alcance	Proporción de todas las unidades de entradas cubiertas por los procesos. Proporción de todas las entradas muestreadas y probadas.
Indisponibilidad	Número de interrupciones de la operación normal del proceso. Frecuencia de las interrupciones de la operación normal del proceso. Tiempo de actividad de la operación normal del proceso.
Efectividad	Número de entradas. Tiempo medio entre entradas. Fracción de entradas que producen una salida.
Eficiencia	Relación de número de salida presentado a los recursos disponibles para este proceso en el uso actual. Relación de proporción de todas las unidades de entradas cubiertas por este proceso para los recursos disponibles para este proceso en el uso actual. Relación de proporción de unidades de entrada muestreadas o probadas para los recursos disponibles para este proceso en el uso actual.
Carga	Proporción de recursos en el uso actual
Calidad	Exactitud, precisión u otras mediciones adecuadas para el propósito de la salida

Tabla 15. Tipos de Métrica ISM3

Especificación de Métricas de Proceso

Para que una métrica este completamente definida, los siguientes ítems deber ser especificados:

Métrica	**Nombre de la métrica.**
Tipo de métrica	Actividad, alcance, indisponibilidad, efectividad, carga, calidad o eficiencia
Descripción de la métrica	Descripción de que está siendo medido
Procedimiento de medición	Como la métrica es medida
Frecuencia de medición	Con que frecuencia las mediciones son tomadas
Estimación de Umbrales	Como los umbrales son calculados
Exactitud de Umbrales	Proporción de verdaderos positivos y verdaderos negativos
Umbrales Actuales	Rango actual de valores considerado normal para la métrica
Valor Meta	Valor mejor posible de la métrica
Unidades	Unidades de medición
Categorías	Nombre y descripción de cada categoría y subdivisión

Métricas de procesos de evaluación de desempeño se utilizan para proporcionar información sobre el desempeño de las prácticas de gestión, incluyendo las siguientes:

- Gestión del Conocimiento
- Implementación
- Operación
    - Pruebas
    - Monitoreo
    - Mejoramiento
    - Planeación

- Evaluación
    - Evaluación
    - Auditoria
    - Certificación
    - Realización de Beneficios

Uso Operacional de Métricas de Proceso

Existen cinco pasos en el uso de métricas:

1. Medición. Las mediciones del valor actual de la métrica es periódica y normalmente se refiere a una ventana.
2. Interpretación. El resultado de un valor medido es evaluado comparando el valor de la medición con un umbral, medición comparable o meta. Los resultados de la interpretación son:
    a. Anomalía
    b. Éxito
    c. Tendencia
    d. Benchmark
3. Investigación. La investigación de las mediciones anormales idealmente termina con la identificación de la causa común.

4. Representación. Visualización adecuada de la métrica es la clave para la interpretación fiable.
5. Diagnóstico. Los administradores deben utilizar los resultados de los pasos anteriores para diagnosticar la situación y analizar las alternativas y sus consecuencias para obtener apropiadas decisiones de negocio.

ISM3 en el contexto del negocio

Contexto del negocio

ISM3 es un marco de trabajo para gestionar la seguridad de la información en el contexto de los objetivos del negocio.

Una organización utilizando ISM3 reconoce que existe una negociación entre seguridad de la información y otros intereses del negocio y se requiere que la gestión de seguridad y del negocio trabajen juntas. Cuando ISM3 es implementado correctamente , la gestión trabaja en colaboración para alcanzar los mismos objetivos, con menos fricción entre la función de seguridad y otras unidades del negocio.

ISM3 aborda la falta de claridad y acuerdo sobre lo que significa en la práctica seguridad, utilizando definiciones operacionales que dicen que se debe lograr, en lugar de las definiciones conceptuales de términos importantes como confidencialidad, disponibilidad e integridad.

Modelo de Seguridad en Contexto

El modelo de seguridad en contexto de ISM3 brinda a los administradores de seguridad una metodología para traducir los resultados para la seguridad en especificaciones técnicas del sistema de seguridad. El modelo se describe en la siguiente figura 18.

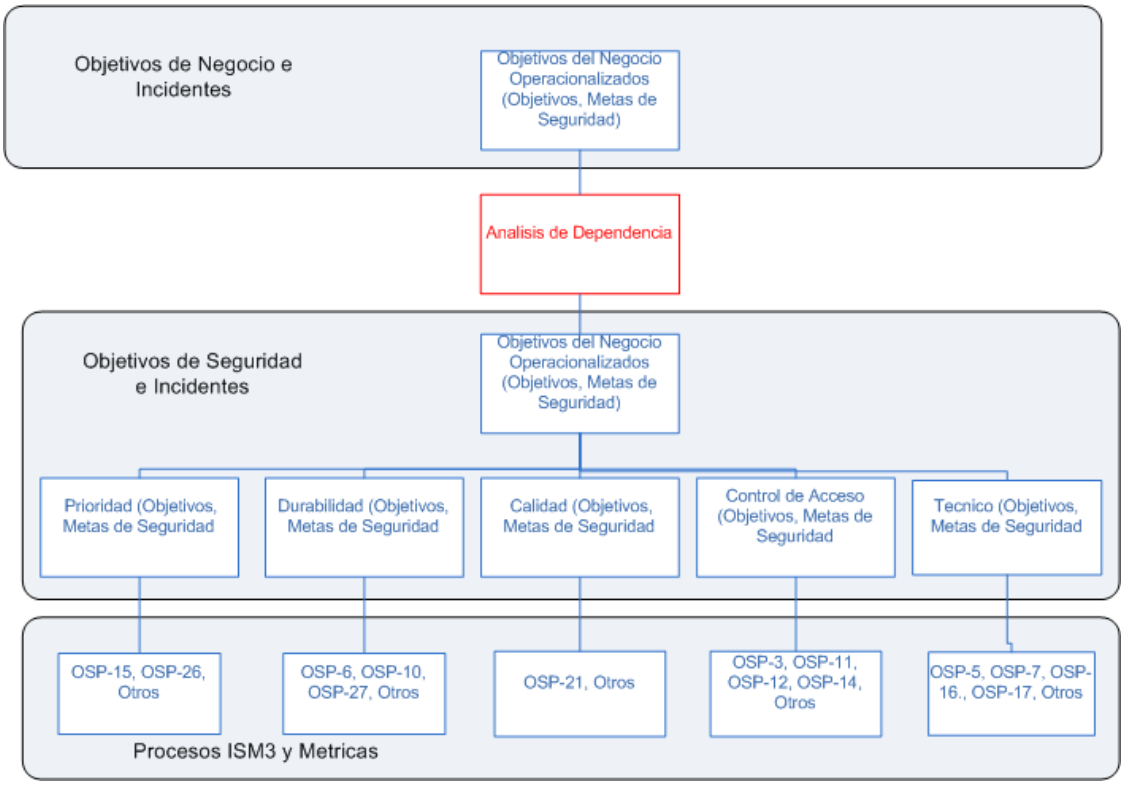


Figura 18. Modelo de Seguridad en Contexto de ISM3

Enfoque Operacional

El enfoque operacional de ISM3 define un incidente como una falla para lograr uno o más de objetivos del negocio y de seguridad acordados en la gestión. Una falla del SGSI ocurre cuando una meta de seguridad es vulnerada. Un estado de seguridad existe cuando continuamente se cumplan todos los objetivos dentro de las tolerancias de las metas de seguridad a pesar de las amenazas.

Cuando objetivos del negocio y objetivos de seguridad están alineados, la seguridad de la información viene a ser el factor clave para el logro común de los objetivos del negocio. El progreso hacia una mejor seguridad es medida en términos de incrementar la predictibilidad de lograr objetivos de seguridad.

Definiciones Operacionales

ISM3 pretende facilitar la comunicación entre la seguridad, TI y la administración. Si bien las Metas de Seguridad son necesariamente específicas y detalladas, el uso de términos operacionales ayuda a remover ambigüedad y la posibilidad de un malentendido

Definición de ISM3 – Seguridad en Contexto

ISM3 define la seguridad como el resultado de cumplir de forma continua o superar un conjunto de objetivos. Debido a que los objetivos del negocio difieren entre organizaciones, el enfoque de la seguridad en contexto hace que la seguridad de ISM3 sea dependiente del contexto.

En la seguridad en contexto, un incidente es una falla de cumplir los objetivos de la organización, los cuales son expresados en objetivos del negocio y objetivos de seguridad.

ISM3 se enfoca en lograr los objetivos del negocio y de seguridad. La protección de activos es importante en la medida en que favorece al logro de los objetivos de seguridad.

Objetivos del Negocio, Objetivos de Seguridad y Metas de Seguridad

Objetivos del Negocio

Cada organización existe para propósitos específicos que requieren un conjunto de objetivos y reunir ciertas obligaciones. Los Objetivos del Negocio van desde objetivos que se aspiran hasta cumplimiento regulatorio. Cada objetivo del negocio en ISM3 es definido operacionalmente.

Objetivos de Seguridad

ISM3 documenta la contribución de la seguridad de la información para alcanzar los objetivos del negocio a través del uso de un análisis de dependencia. La salida del análisis de dependencia es una lista de los objetivos de seguridad que forman la base para el diseño, implementación y monitoreo del SGSI.

Metas de seguridad

Todos los Objetivos (Negocio y Seguridad) ISM3 deben incluir sus metas de seguridad. Esta es la desviación máxima del resultado deseado que la administración tolera antes de tomar una acción correctiva.

Las metas de seguridad son normalmente definidas en términos de frecuencia de ocurrencia y un umbral de costo, como el impacto en el negocio permitido de no cumplir con los objetivos refleja la disyuntiva frente a otras prioridades y objetivos. Las metas de seguridad muestran que es lo que la organización espera de su inversión de seguridad.

Interpretación ISM3 de Incidentes, Éxito y Fallo

ISM3 utiliza objetivos de negocio y seguridad, metas de seguridad como el criterio para determinar ambos: ocurrencia de incidentes y el éxito general de una Gestión de Seguridad de la Información.

Un incidente se reconoce cada vez que un objetivo de negocio o la seguridad no se cumple.

ISM3 define el éxito como el logro de la meta de la seguridad relativa a ese objetivo, no si un incidente se ha o no se ha producido.

ISM3 define el fracaso como lo contrario de éxito; es decir, uno o más objetivos de negocio o los objetivos de seguridad no se cumplieron.

Modelo de Proceso ISM3

En el contexto ISM3, seguridad es el resultado de un proceso. Entre mejor el proceso de seguridad, mejor es la protección que se consigue a partir de los recursos disponibles.

Gestión de Seguridad – Fundamentos de ISM3

Para manejar algo significa definir y alcanzar objetivos, mientras se optimizan el uso de recursos. Las actividades de gestión normalmente incluyen los requerimientos para planificar, dirigir, controlar y coordinar (ver figura 19).

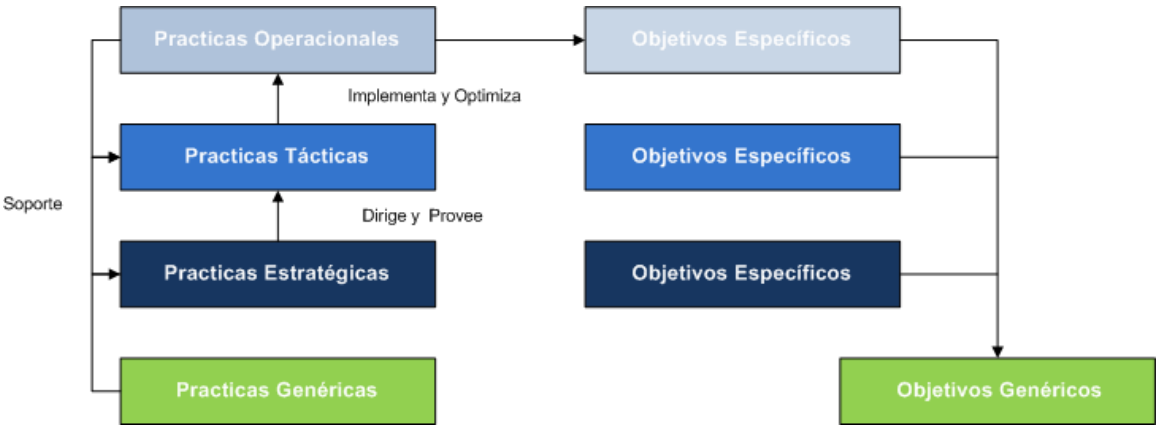


Figura 19. Niveles de Gestión de Seguridad ISM3

Figura 20. Estructura de Reportes de Niveles de Gestión de Seguridad ISM3

Tercerización

Introducción

Muchas compañías consideran la tercerización de la gestión de la seguridad como una solución apropiada para su modelo de negocio, ya sea como servicio completo o como la selección de un servicio.

Acuerdo de Nivel de Servicio

Un Acuerdo de Nivel de Servicio (del inglés, SLA) es un acuerdo de calidad entre un proveedor y el cliente, especificando mediante un conjunto de métricas. SLAs son utilizadas frecuentemente para monitorear y mejorar la calidad del servicio provisto por un tercero.

Lineamientos

Para implementaciones del marco de trabajo, ISM3 recomienda doce lineamientos en servicios tercerizados. Como por ejemplo: El servicio debe ser definido en un contrato y firmado por los representantes legales de ambas partes, entre otros.

Implementación de ISM3

Arriba hacia Abajo (Top-Down) o Desde la Base (Bottom-Up)

Existen dos escenarios principales para implementar ISM3:

- En la implementación Arriba hacia Abajo (Top-Down), la dirección ejecutiva a nivel CEO decide implementar ISM3 y asigna los recursos adecuados. En este escenario, los administradores de seguridad/ líderes de proyecto responsables de la implantación trabajan cerca de la dirección ejecutiva para lograr los objetivos de seguridad acordados.
- En la implementación desde la base (Bottom-Up), un gerente de seguridad de la información o un gerente dentro de la organización decide utilizar los recursos existentes para desarrollar una implementación piloto de ISM3 o una implementación a nivel de dominio ISM3. El objetivo puede ser mejorar la alineación y la gestión de los procesos de seguridad de la información o demostrar el valor y Retorno de Inversión (del inglés, ROI) que ISM3 puede rendir como medida de ahorro.

No hay una solución única para todos

Cada organización tiene un contexto particular y se ve limitada por los recursos disponibles. Las organizaciones utilizando ISM3 hacen uso de proceso de toma de decisiones para elaborar un subconjunto de procesos que van desde la jerarquía total de procesos disponibles. Los procesos se pueden ejecutar varias veces en una organización bajo diferentes dueños de procesos o en diferentes dominios gestionados de TI.

Seleccionando los Procesos a Implementar

La selección de proceso depende:

- Recursos disponibles
- Tamaño y complejidad de la organización
- Requerimientos para estar conforme a cualquier certificación
- Regulación aplicable y requerimientos de auditoria
- La tolerancia del riesgo de la organización y su posible sensibilidad para perdida financiera y perdida de reputación
- Si los elementos de riesgo o pérdida se puede reducir por el seguro o la contratación externa

Procesos fundamentales para una implementación ISM3 top-down

Los siguientes procesos son considerados esenciales para cualquier SGSI en funcionamiento y deben ser considerados como conjunto de procesos inicial para cualquier implantación Top-Down:

- GP-1: Gestión del Conocimiento
- GP-3: Diseño de SGSI y Evolución
- SSP-1: Reportar a los grupos de interés
- SSP-2: Coordinación
- SSP-6: Asignar Recursos para la Seguridad de la Información
- TSP-1: Reportar a Gestión Estrategica
- TSP-2: Administrar los Recursos Asignados
- TSP-3: Definir Metas de Seguridad
- TSP-4: Gestión del Nivel de Servicio
- OSP-1: Reportar a la Gestión Táctica
- OSP-5: Aplicación de Parches Gestionados por TI
- OSP-11: Control de Acceso
- OSP-16: Segmentación y Gestión de Filtrado
- OSP-17: Gestión de Protección contra Malware
- OSP-10: Gestión de Respaldos
- OSP-21: Evaluación de Calidad de Información y Cumplimiento

Guía sobre el papel de los grupos clave de los procesos ISM3

La guía esta presentada en tablas que agrupan un número de procesos ISM3, estimados por la magnitud de la inversión requerida y el beneficio esperado en términos de reducción de riesgos (ver tabla 16). Estos agrupamientos indican o especifican:

- La relación costo/beneficio que se podría conseguir en una implementación típica
- Conjuntos de procesos asociados
- Las entradas de uno son las salidas de otro
- Están lógicamente relacionados

	Baja Inversión	Mediana Inversión	Alta Inversión
Alto Beneficio	OSP-12: Registro de Usuario SSP-4: Define las reglas de la división de funciones TSP-6: Arquitectura de Seguridad GP-2: SGSI y Auditoria del Negocio	OSP-14: Gestión para Protección de Ambiente Físico OSP-7: Endurecimiento Gestionado por TI OSP-8: Control de Ciclo de Vida de Desarrollo de Software OSP-19: Auditorias Técnicas Internas	OSP-4: Control de Cambios Gestionado por Sistemas de Información de TI OSP-9: Medidas de Seguridad en Control de Cambios OSP-26: Confiabilidad Reforzada y Gestión de Disponibilidad
Mediano Beneficio	TSP-11: Concientización de Seguridad TSP-8: Seguridad de	OSP-3: Gestión de Inventario OSP-2: Adquisición de	OSP-15: Gestión de Continuidad de Operaciones

	Baja Inversión	Mediana Inversión	Alta Inversión
	Personal TSP-9: Formación de Personal de Seguridad	Seguridad OSP-6: Compensación Gestionado por TI OSP-27: Gestión de Archivado	OSP-20: Emulación de Incidentes
Bajo Beneficio	TSP-10: Proceso Disciplinario TSP-13: Gestión de Seguros	OSP-22: Monitoreo de Alertas OSP-28: Detección y Análisis de Eventos Externos OSP-23: Detección y Análisis de Eventos Internos OSP-24: Manejo de Incidentes y Potenciales Incidentes OSP-25: Forense	TSP-7: Revisión de Antecedentes TSP-14: Operaciones de Información

Tabla 16. La variación de rendimiento de la inversión de los diferentes procesos

Implementación de Arriba hacia Abajo (Top-Down)

Los siguientes pasos deben ser tomados para implementación inicial Top-Down:

1. Obtener compromiso de la alta dirección
2. Nombrar un CISO (del Inglés, Chief Infortmation Security Officer) y conformar el Comité Ejecutivo de Seguridad y el Comité de Seguridad de la Información
3. Determinar la meta ISM3 de madurez y capacidad (si las hay)
4. Determinar algún requerimiento regulatorio
5. Determinar requerimientos adicionales de certificación
6. Evaluar / Analizar Brechas entre el SGSI actual y SGSI basado en ISM3
7. Establecer el GP-1: Gestión del Conocimiento
8. El Comité Ejecutivo de Seguridad determina la estrategia de implementación
9. Establecer los procesos de Gestión Estratégica
10. Establecer los procesos seleccionados de la Gestión Táctica
11. Determinar las métricas para cada proceso dependiendo del nivel de capacidad buscado
12. Establecer o Tercerizar los Procesos Operacionales de la gestión de seguridad de la información
13. Asignar responsabilidades
14. Diseñar y documentar (usando GP-1) SGSI basado en ISM3
15. Crear y publicar las Políticas de Seguridad de la Información usando GP-3
16. Entrenar a los administradores y usuarios en sus responsabilidades en SGSI usando TSP-9
17. Revisar la operación de todos los procesos usando TSP-4
18. Revisar las Metas de Seguridad usando TSP-3
19. Operar el SGSI
20. Definir y afinar los umbrales las métricas de los procesos usando TSP-4

21. Auditar el SGSI periódicamente usando GP-2
22. Opcionalmente, certificar el SGSI según los requisitos de la certificación
23. Mantener y mejorar el SGSI usando GP-3

Implementación desde la Base (Bottom-Up)

Los siguientes pasos deben ser tomados para implementación inicial Bottom-Up:

1. Establezca el GP-1
2. Aplique las políticas y conocimiento existente de la organización para elaborar los objetivos de seguridad
3. Clasifique los repositorios y servicios de acuerdo a los objetivos de seguridad; nombre dueños de sistemas
4. Establezca las metas de seguridad para cada dominio gestionado por TI
5. Selecciones procesos operacionales apropiados para cada dominio gestionado por TI
6. Determine métricas para cada proceso dependiente del nivel de capacidad buscado
7. Establezca procesos de gestión de seguridad de información operacionales
8. Asigne responsabilidades
9. Diseñe y documente los procesos (usando GP-1)
10. Revise la operación de todos los procesos usando TSP-4
11. Revise las metas de seguridad usando TSP-3
12. Opere el SGSI
13. Defina y afine los umbrales las métricas de los procesos usando TSP-4
14. Mantenga y mejore el SGSI usando GP-3

Ejemplos de Niveles de Madurez ISM3

Las siguientes tablas especifican la capacidad y la composición de los procesos de ejemplos de niveles de madurez. Ellos ofrecen sugerencias en como iniciar el uso de ISM3.

Nota:

- Los términos “Gestionado” y “Optimizado” se definieron anteriormente.
- Las tablas ofrecen sugerencias como guía; Ellos pueden ser modificados por los requerimientos de la organización.

Un nivel de madurez es determinado por el proceso de composición y la capacidad de cada proceso.

- Si dos SGSIs tienen la misma composición de proceso y uno de ellos tiene capacidad más alta, será considerado con más madurez.
- Si dos SGSIs tienen el mismo nivel de capacidad y uno tiene más procesos que el otro, será considerado con más madurez.

General

	Nivel 1	**Nivel 2**	**Nivel 3**	**Nivel 4**	**Nivel 5**
GP-1: Gestión del	Gestionado	Gestionado	Gestionado	Gestionado	Optimizado

	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
Conocimiento					
GP-2: SGSI y Auditoria del Negocio	Gestionado	Gestionado	Gestionado	Gestionado	Optimizado
GP-3: Diseño de GSI y Evolución	Gestionado	Gestionado	Gestionado	Gestionado	Optimizado

Gestión Estratégica

	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
SSP-1: Reportar a los grupos de interés	Gestionado	Gestionado	Gestionado	Gestionado	Optimizado
SSP-2: Coordinación	Gestionado	Gestionado	Gestionado	Gestionado	Optimizado
SSP-4: Define las reglas de la división de funciones				Gestionado	Optimizado
SSP-6: Asignar Recursos para la Seguridad de la Información	Gestionado	Gestionado	Gestionado	Gestionado	Optimizado

Gestión Táctica

	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
TSP-1: Reportar a Gestión Estratégica	Gestionado	Gestionado	Gestionado	Gestionado	Optimizado
TSP-2: Administrar los Recursos Asignados	Gestionado	Gestionado	Gestionado	Gestionado	Optimizado
TSP-3: Definir Metas de Seguridad y Objetivos de Seguridad	Gestionado	Gestionado	Gestionado	Gestionado	Optimizado
STSP-4: Gestión del Nivel de Servicio			Gestionado	Gestionado	Optimizado
TSP-6: Arquitectura de Seguridad		Gestionado	Gestionado	Gestionado	Optimizado
TSP-13: Gestión de Seguros				Gestionado	Optimizado
TSP-7: Revisión de				Gestionado	Optimizado

	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
Antecedentes					
TSP-8: Seguridad de Personal				Gestionado	Optimizado
TSP-9: Formación de Personal de Seguridad			Gestionado	Gestionado	Optimizado
TSP-10: Proceso Disciplinario		Gestionado	Gestionado	Gestionado	Optimizado
TSP-11: Concientización de Seguridad		Gestionado	Gestionado	Gestionado	Optimizado
TSP-14: Operaciones de Información					Optimizado

Gestión Operacional

	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
OSP-1: Reportar a la Gestión Táctica	Gestionado	Gestionado	Gestionado	Gestionado	Optimizado
OSP-2: Adquisición de Seguridad		Gestionado	Gestionado	Gestionado	Optimizado
OSP-3: Gestión de Inventario			Gestionado	Gestionado	Optimizado
OSP-4: Control de Cambios Gestionado por Sistemas de Información de TI		Gestionado	Gestionado	Gestionado	Optimizado
OSP-5: Aplicación de Parches Gestionados por TI	Gestionado	Gestionado	Gestionado	Gestionado	Optimizado
OSP-6: Compensación Gestionado por TI		Gestionado	Gestionado	Gestionado	Optimizado
OSP-7: Endurecimiento Gestionado por TI		Gestionado	Gestionado	Gestionado	Optimizado
OSP-8: Control de Ciclo de Vida de Desarrollo de Software			Gestionado	Gestionado	Optimizado
OSP-9: Medidas de Seguridad en Control de		Gestionado	Gestionado	Gestionado	Optimizado

	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
Cambios					
OSP-16: Segmentación y Gestión de Filtrado	Gestionado	Gestionado	Gestionado	Gestionado	Optimizado
OSP-17: Gestión de Protección contra Malware	Gestionado	Gestionado	Gestionado	Gestionado	Optimizado
OSP-11: Control de Acceso		Gestionado	Gestionado	Gestionado	Optimizado
OSP-12: Registro de Usuario		Gestionado	Gestionado	Gestionado	Optimizado
OSP-14: Gestión para Protección de Ambiente Físico		Gestionado	Gestionado	Gestionado	Optimizado
OSP-10: Gestión de Respaldos	Gestionado	Gestionado	Gestionado	Gestionado	Optimizado
OSP-26: Confiabilidad Reforzada y Gestión de Disponibilidad				Gestionado	Optimizado
OSP-15: Gestión de Continuidad de Operaciones			Gestionado	Gestionado	Optimizado
OSP-27: Gestión de Archivado				Gestionado	Optimizado
OSP-19: Auditorias Técnicas Internas		Gestionado	Gestionado	Gestionado	Optimizado
OSP-20: Emulación de Incidentes			Gestionado	Gestionado	Optimizado
OSP-21: Evaluación de Calidad de Información y Cumplimiento				Gestionado	Optimizado
OSP-22: Monitoreo de Alertas		Gestionado	Gestionado	Gestionado	Optimizado
OSP-28: Detección y Análisis de Eventos Externos				Gestionado	Optimizado
OSP-23: Detección y Análisis de Eventos Internos				Gestionado	Optimizado
OSP-24: Manejo de Incidentes y Potenciales			Gestionado	Gestionado	Optimizado

	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
Incidentes					
OSP-25: Forense				Gestionado	Optimizado

2.3.5 IS2ME: Seguridad de la Información a la Mediana Empresa (Information Security to Medium Enterprise) (Linares & Paredes, 2007)

Antecedentes

Existen un número reducido de medianas empresas (empresas aproximadamente con un número menor de 500 empleados) las cuales representan el 90% del total de las empresas del mundo, las cuales tienen niveles muy altos de implantación de seguridad de la información mientras que la mayoría tiene falencias importantes en el conocimiento de seguridad de la información, en particular existe una marcada falta de madurez en las organizaciones de este tipo en lo que se refiere a la seguridad de la información.

Normalmente no existe la estructura organizativa adecuada, la misma persona responsable de TI asume la responsabilidad de la seguridad de la información, pero con falta de formación e implementaciones básicas y la mayoría de casos responden a problemas puntuales. A esto se le suma la labor diaria "día a día", la cual impide tener una visión integrada o realizar una adecuada planificación y gestión. Todo esto impactando negativamente a la organización.

Introducción

La organizaciones presentan requisitos indispensables como la pronta disponibilidad de resultados que disminuyan el riesgo existente, la implantación de medidas de seguridad críticas y la presentación de un plan de acción, que permita tanto a la alta dirección como al responsable de seguridad, identificar los recursos necesarios y cuál debe ser la ruta a seguir para incorporar la seguridad como requisito de los procesos de la organización. Este reto, el área de seguridad o la persona responsable, lo puede abordar siguiendo los estándares o metodologías existentes como es el caso de la ISO 27001 y de esa manera iniciar un proceso de implementación de un SGSI, este proceso se hace al pie de la letra se vuelve complejo debido principalmente a la falta de concientización de la alta dirección y a la no existencia de una bases mínimas en los que respecta a la seguridad de la información. Este tipo de enfoque completo y de fiel seguimiento muchas veces no es del todo requerido por las organizaciones debido a que estas necesitan o requieren resultados inmediatos y prácticos a corto plazo.

Es este punto donde surge la necesidad de una metodología que se adapte a este escenario y es donde IS2ME, Information Security to the Medium Enterprise (Seguridad de la Información a la Mediana Empresa) se presenta como la alternativa y aproximación para la ruta a seguir hacia la implantación de la seguridad de la información de organizaciones cuyo modelo de seguridad aun no es maduro y requieren llevar a cabo la implementación de la seguridad de la información y de su sistema de gestión de una forma eficiente, eficaz y práctica. Mitigando de esta manera el riesgo en la organización a corto plazo y al mismo tiempo se pueda iniciar la ruta hacia el cumplimiento de los estándares deseados.

IS2ME tiene como uno de sus objetivos, acercar la seguridad de la información a las medianas y pequeñas empresas, reducir el nivel de riesgo, aumentando el valor y rentabilidad; como resultado se eleva el nivel económico de las organizaciones de este tipo.

Objetivos

- Disminuir de forma rápida el riesgo asumido por la organización en lo que respecta a seguridad de la información. Esto a través del establecimiento de un marco de implantación de las medidas técnicas y organizativas necesarias.
- Incorporar la seguridad de la información en la cultura de la organizacional.
- Identificar el estado actual de la seguridad de la información de la organización, las acciones de mejora y plan de acción para implementación de estas acciones.
- Proponer un método claro y definido de acercamiento de las pequeñas y medianas empresas al cumplimiento de los estándares deseados.
- Sentar las bases para posterior desarrollo en profundidad hacia el cumplimiento e implantación total del SGSI según las normas existentes, si así se requiere.

Características clave

- Metodología adaptable a pequeñas y medianas organizaciones y de resultados a corto plazo
- Mitigación del riesgo a corto plazo
- Gestión de la seguridad de la información de una forma eficiente, eficaz y práctica
- Marco que ayuda a la organización a iniciar la ruta hacia el cumplimiento de los estándares deseados

Ventajas o beneficios

- Se puede aplicar a pequeñas y medianas organizaciones
- Versión en español directa de sus autores
- Implementación seguridad de la información a corto plazo y con utilización razonable de recursos

Descripción de método IS2ME

IS2ME se inicia generalmente evaluando la seguridad de la información de la organización mediante la recolección de información a través de entrevistas, pruebas de campo y análisis técnicos. A continuación se presenta figura 21 con la descripción general del proceso.

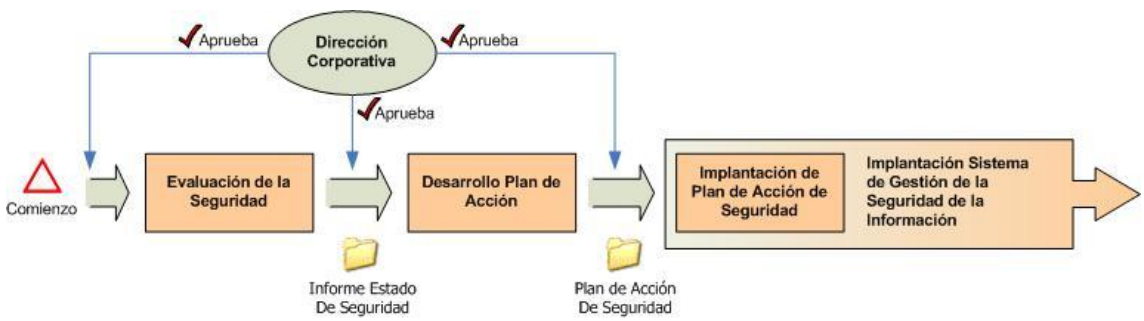


Figura 21. Descripción general de Proceso de IS2ME

En la elaboración de IS2ME se ha seguido un enfoque holístico y sumamente practico que permite al usuario una aplicación sencilla e inmediata mediante el seguimiento de fases secuenciales bien diferenciadas que se muestran en la siguiente figura 22 y se describen a continuación:

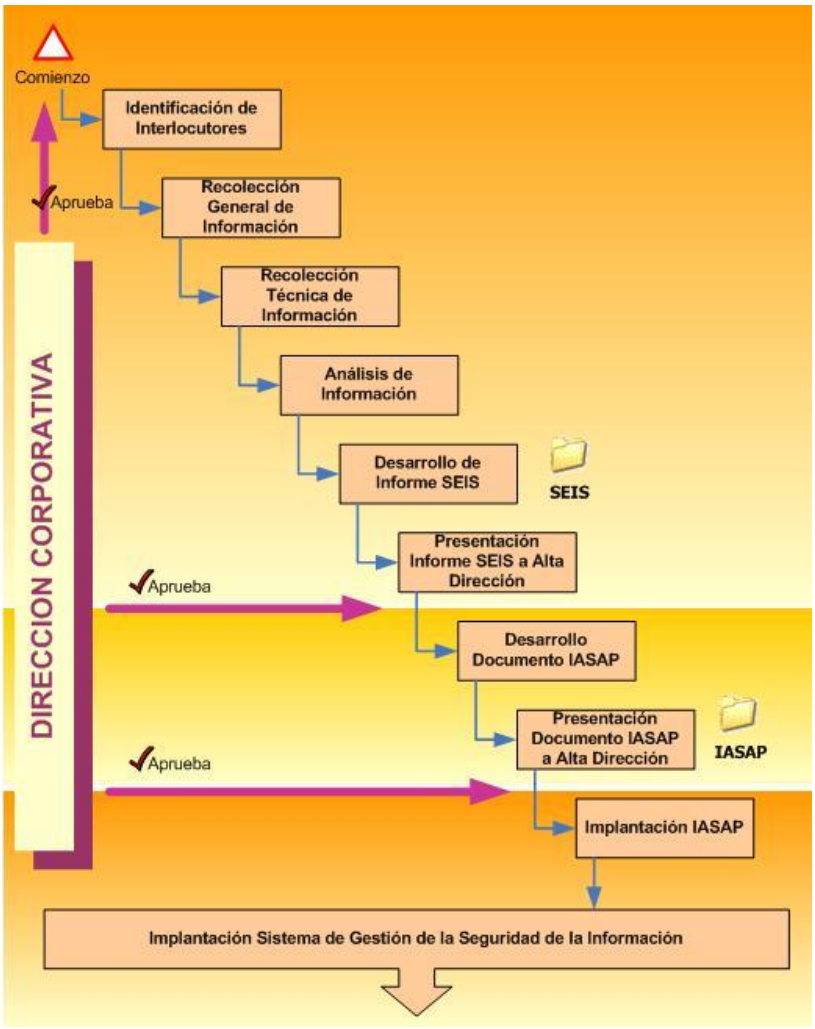


Figura 22. Fases IS2ME

Identificación de Interlocutores

Objetivo: Identificación de interlocutor (o interlocutores) válidos en la organización y planificación de su disponibilidad por parte de la organización.

La función es ser interlocutor entre el equipo de trabajo que está desarrollando el estudio y la organización. Tanto la organización como el equipo de trabajo deben firmar autorizaciones y acuerdos según corresponda. La organización debe firma por escrito la autorización para realizar pruebas y para la obtención de la información necesaria para la realización de las tareas

requeridas. Por otro lado el equipo de trabajo debe firmar acuerdo de confidencial, la cual es la garantía de la organización de la no difusión ni la utilización de la información tratada.

Recolección General de Información

Objetivo: Obtención de todo tipo de información mediante entrevistas, revisión de documentación y métodos análogos referente a seguridad de la información, que deberá incluir información técnica, organizativa y de cumplimiento.

En esta fase inicial se recolectará la información necesaria de la organización que es la entrada de las posteriores baterías de pruebas y análisis técnicos necesarios. Previamente a la presencia del equipo de trabajo en la organización, podrá facilitarse al interlocutor seleccionado un cuestionario que deberá ser remitido debidamente lleno al equipo de trabajo para llevar a cabo la recolección de información de la forma más eficiente posteriormente. Este formulario podrá contener cuestiones técnicas, organizativas sobre la organización y de cumplimiento con el objetivo de minimizar el tiempo empleado tanto por la organización como por el equipo de trabajo al momento de realizar las visitas.

Recolección Técnica de Información

Objetivo: Obtención de todo tipo de información mediante diversos métodos técnicos y empíricos en una muestra representativa de los sistemas y dispositivos de la organización.

En esta fase se procederá a identificar los sistemas objeto de estudio para luego realizar una serie de análisis técnicos con el fin de conocer de forma precisa cuál es su estado real desde un punto de vista de seguridad técnica. Mediante estos análisis seremos capaces de detectar problemas de seguridad, existentes o potenciales, que puedan afectar a la integridad de los sistemas de la organización, además de a su funcionamiento o rendimiento.

A continuación se enumeran los distintos puntos que deberán ser abordados durante la recolección técnica de información:

- Enumeración y Caracterización
- Análisis de Tráfico
- Análisis de Vulnerabilidades Sistemas y Aplicaciones
- Análisis remoto
- Análisis local
- Revisión de configuraciones
- Visibilidad externa
- Direccionamiento público
- Nombres de dominio y DNS
- Filtrado de documentación
- Otros análisis técnicos

Análisis de Información

Objetivo: Estudio y análisis de la información recolectada en las fases anteriores en base a códigos de mejores prácticas, estándares, normas, metodologías, conocimiento y experiencia del equipo de trabajo.

En esta fase se realiza el análisis de toda la información recogida y situaciones existentes, estudiando las posibles debilidades en seguridad de la información de los productos, diseños de red, accesos a información o procesos organizativos implementados, entre otras; tomando como base fuentes como los códigos de buenas prácticas existentes aplicables a los distintos sistemas y procesos analizados, metodologías y estándares (como ISO 27001) de recomendable u obligado cumplimiento, legislación y normativas internas aplicables, además de bases de conocimiento existentes sobre los distintos sistemas o productos analizados y la experiencia y conocimiento del equipo de trabajo encargado del proyecto. En el desarrollo de este análisis es importante la experiencia y conocimiento del equipo de trabajo en las distintas áreas de la seguridad de la información.

Desarrollo de Informe SEIS (State of Enterprise Information Security, Estado de la Seguridad de la Información de la Compañía)

Objetivo: Elaboración del informe de estado de la seguridad de la información en la compañía que recogerá en un único documento una imagen de la situación actual de la organización en lo que a implantación de medidas técnicas y organizativas de la seguridad de la información se refiere.

Del resultado de la información obtenida en la Recolección Técnica de información y su respectivo análisis, se debe desarrollar el informe SEIS (State of Enterprise Information Security).

Los objetivos del informe son:

- Proporciona una visión global y detallada del estado de seguridad de la información en la organización
- Señalar cuales son los aspectos mejorables que atañen a la seguridad de la información así como proponer acciones correctivas priorizando de acuerdo importancia que tengan para la organización

A continuación se listan los apartados que componen el informe SEIS:

- Descripción del estado actual
- Análisis y Recomendaciones Técnicas
- Conclusiones y Propuestas de acción
- Medidas de Seguridad y Controles Recomendados
- Resumen Ejecutivo

Presentación de Informe SEIS a Alta Dirección

Objetivo: Presentación del Informe de Estado de Seguridad de la Información de la compañía a la alta dirección, suponiendo ello un hito para la asunción de la seguridad como un requisito de negocio más en la cultura organizacional de la compañía.

Debe realizarse una presentación del informe SEIS a la alta dirección para lo que se debe identificar cuáles son los mensajes claves que se desean transmitir, siempre desarrollando esos mensajes en un lenguaje entendible para este nivel de personas de la organización, no tanto técnica, sino del negocio y de riesgos financieros, entre otros.

La presentación deberá estructurarse adecuadamente, se recomienda un esquema similar al siguiente:

- Muy breve introducción sobre seguridad de la información
- Descripción del estudio realizado y motivación del mismo
- Estado actual de la organización
- Ejemplos reales de hallazgos, problemas y/o vulnerabilidades existentes
- Recomendaciones
- Acciones inmediatas requeridas
- Conclusiones

Se recomienda que en la sección del estado actual y las conclusiones se indique clara y explícitamente el nivel de riesgo asumido por la organización mediante afirmaciones breves y concisas.

La duración depende de la dimensión de la organización, la naturaleza de la información a presentar y otras consideraciones, pero se recomienda al menos 1 hora y máximo 2 horas.

El resultado debe materializarse en el apoyo y compromiso explícito de la alta dirección en el desarrollo de la continuación del proyecto y en la aprobación del informe SEIS que suponga la aprobación para comenzar el desarrollo del documento IASAP (Plan de Acción de Seguridad de la Información, Information Assurance and Security Action Plan).

Desarrollo del Documento IASAP (Information Assurance and Security Action Plan, Plan de Acción de Seguridad y Protección de la Información)

Objetivo: Elaboración del documento Plan de Acción de Seguridad y Protección de la Información como base para la posterior implantación de acciones correspondientes en la organización y elaboración de los Planes de Seguridad de la Organización.

Para el diseño o desarrollo de muchos sistemas de información, en algunas ocasiones, no se tienen en cuenta requisitos o características de seguridad adecuadas. Debido a ello la seguridad que puede lograrse por medios técnicos es limitada y debe ser apoyada por una gestión y procedimientos adecuados, participación completa todo el personal de la organización y en algunos casos de proveedores y usuarios o clientes.

En este sentido es importante que la organización identifique sus requisitos de seguridad mediante la evaluación de los riesgos, identificar requisitos legales, normativos, reglamentarios y contractuales que debe cumplir. Además de los principios, objetivos y requisitos para el procesamiento de la información que ha desarrollado para respaldar sus operaciones.

Con los requisitos de seguridad identificados, se debe seleccionar e implementar acciones y medidas de seguridad adecuadas para reducir los riesgos a un nivel aceptable. En el documento IASAP debe documentarse los recursos necesarios para la implementación de las acciones y medidas y también su planificación o valoración económica cuando corresponda. Este documento conformara el Plan de Acción de Seguridad de la Información de la organización.

A continuación una información mínima que debe contener el documento:

- Desarrollo técnico, completo y en detalle de la acción
- Planificación completa y detallada de cada acción
- Identificación de recursos humanos necesarios
- Valoración económica en aquellos casos que pueda realizarse
- Ofertas de proveedores en aquellas acciones que requieran de un tercero

Las acciones a incluir en el IASAP dependen de las medidas de seguridad que la organización tenga implementada y del grado de permeabilidad de la seguridad de la información en la cultura organizacional, pero al menos se sugieren las siguientes:

- Mejora de la estructura organizativa de la compañía (establecimiento de comité de seguridad, asignación de responsabilidades, etc.)
- Posible externalización de algunas funciones TI
- Desarrollo y difusión de políticas de seguridad y procedimientos asociados
- Mejoras en las plataformas de sistemas o en el centro de proceso de datos
- Mejoras en la seguridad de los dispositivos de comunicaciones (redes inalámbricas, WAN, LAN, segmentación de redes, etc.)
- Análisis de vulnerabilidades
- Desarrollo del proceso de gestión de la continuidad del negocio
- Análisis de riesgos
- Desarrollo del plan de contingencia TI
- Plan de formación
- Otros

Presentación del Documento IASAP a Alta Dirección

Objetivo: Presentación del Plan de Seguridad y Protección de la Información a la Alta Dirección para su aprobación, sentando así la base para su posterior implantación.

Una vez finalizado el documento IASAP debe ser presentado y defendido ante la alta dirección para que este pueda ser aprobado. Una vez aprobado el documento IASAP por la alta dirección supone un hito crucial en el compromiso de la organización en la inclusión de la seguridad de la

información en todos sus procesos, ya que es el comienzo del Plan de Acción de Seguridad de la Información según las características, planificación y estimación de recursos humanos y económicos correspondientes.

En este punto la alta dirección contara con toda la información para valorar los esfuerzos que se deberán tomar para cumplir los objetivos de mitigación de los riesgos y mejora de los niveles de seguridad, analizando la conveniencia de los plazos y acciones propuestas en el documento IASAP y de ser necesario ajustándolos de acuerdo otras consideraciones adicionales por la visión global que alta dirección cuenta.

Además de todas las mejoras aportadas en el área de la seguridad, la institucionalización del documento IASAP como marco de implementación de las acciones indicadas se puede tomar como una base para establecer una política de cumplimiento de objetivos a distintos niveles de la organización desde las distintas direcciones, áreas o departamentos, hasta el establecimiento de objetivos individuales asociados a distintas personas o roles existentes.

Implantación de IASAP

Objetivo: Desarrollo e Implantación del Plan de Acción de Seguridad y Protección de la Información según la planificación propuesta en el mismo.

Una vez aceptado el documento IASAP por la alta dirección, se debe iniciar la implantación de las diferentes tareas identificadas en el Plan de Acción de Seguridad de la Información. Para esta implantación no es necesario que el equipo de desarrollo de IS2ME la ejecute, si es importante que el equipo pueda realizar acciones de seguimiento y coordinación con el fin de asegurar que los objetivos sean cumplidos y adecuadamente implantados.

Para realizar la implantación de IASAP, se desarrollará un plan de proyecto de coordinación que debe incluir:

- Adquisición/Asignación de recursos necesarios
- Seguimiento
- Reuniones de Revisión

2.4 Definición de Términos Básicos

Marco de trabajo: Un marco es una estructura conceptual básica usada para resolver y responder a temas complejos.

Madurez: Indica el grado de confiabilidad o dependencia que el negocio puede tener en un proceso, al alcanzar las metas y objetivos deseados.

Metodología: Hace referencia al conjunto de procedimientos racionales utilizados para alcanzar una gama de objetivos que rigen una investigación. Alternativamente puede definirse la metodología como el estudio o elección de un método pertinente para un determinado objetivo.

Modelo: Un modo de describir un conjunto de componentes y de cómo esos componentes se relacionan.

Modelo de madurez: Un modelo que contiene los elementos esenciales de procesos eficaces para una o más áreas de interés y describe un camino de mejora evolutivo desde procesos inmaduros y ad hoc hasta procesos maduros y disciplinados con una mejora en la eficacia y en la calidad.

Nivel de madurez: Nivel de la mejora de procesos, dominios o programas en un conjunto predefinido de criterios en las que se alcanzan todas las metas de ese conjunto.

Seguridad de la Información: según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Genérico: Que es general o se refiere a un conjunto de elementos del mismo género.

Metodología: hace referencia al conjunto de procedimientos racionales utilizados para alcanzar una gama de objetivos que rigen una investigación científica, una exposición doctrinal o tareas que requieran habilidades, conocimientos o cuidados específicos.

Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran

CAPITULO 3: MARCO METODOLOGICO

3.1 Nivel de Investigación

La definición de investigación es como un conjunto de procesos sistemáticos, críticos y empíricos que se aplican al estudio de un fenómeno (Roberto Hernández Sampieri, 2010).

La metodología hace referencia al conjunto de procedimientos racionales utilizados para alcanzar una gama de objetivos que rigen una investigación. Alternativamente puede definirse la metodología como el estudio o elección de un método pertinente para un determinado objetivo.

Basado en el tipo de estudio a realizar que tiene como objetivo proponer un marco de trabajo genérico que permita medir la madurez de la seguridad de la información, la investigación será considerada de modalidad proyectiva y un proceso de investigación cualitativo, definiéndose por investigación proyectiva aquella que consiste en la elaboración de una propuesta de un plan, programa o de un modelo para solucionar problemas o necesidades de tipo práctico, ya sea de un

grupo social, institución, una área en particular del conocimiento, partiendo de un diagnóstico preciso de las necesidades del momento, los procesos explicativos o generadores involucrados y las tendencias futuras. Esta propuesta se involucra los procesos, enfoques, métodos y técnicas. Será un proceso de investigación cualitativa se planteará un problema cualitativo una definición inicial del contexto. Se ha elegido el proceso cualitativo porque la investigación no será lineal, sino iterativo o recurrente. Además, se plantean los objetivos, el alcance, la justificación de manera cualitativa que tengan como características que sean abiertas y expansivas.

3.2 Diseño de Investigación

Este estudio proyectivo intenta proponer soluciones a una situación determinada. Involucra explorar, describir, explicar y proponer alternativas de cambio, más no necesariamente ejecutar la propuesta, como es el caso de esta investigación "Proponer un marco de trabajo genérico que permita medir la madurez de la seguridad de la información". Se debe destacar, por otra parte que la investigación de campo con el objetivo de obtener datos relevantes, que evalúen las condiciones de las organizaciones en cuanto a modelos de madurez de la seguridad de la información, deberá ser en razón de la importancia y conocimiento. La investigación de campo se debe de entender como la recolección de datos directamente de la realidad donde ocurren los hechos sin manipular y controlar.

En esta investigación se realizará como primera fase una investigación documental exploratoria de artículos científicos y fuentes secundarias como libros, tesis, revistas científicas e indexadas para identificar la presencia de estudios descriptivos y obtener un conocimiento general y detallado sobre la temática propuesta, identificar los conceptos claves, los métodos o procesos empleados, para ello se hará uso de técnicas como análisis de contenido con el uso de cuadros comparativos, exploración de información bibliográfica y el diferencial semántico[3]. Como resultado se obtendrá el marco teórico del estudio, donde se describirá cada modelo que cumpla ciertos criterios de estudio, las ventajas y desventajas de cada una de ellas.

La siguiente fase será descriptiva para analizar la situación actual sobre cómo se logra implementar modelos de madurez en las organizaciones, identificando las necesidades de cambio que faciliten la implementación, para ello se hará un estudio a través de recolección de datos siendo un procedimiento estandarizado que se utiliza en el ámbito de la ciencia y la investigación, se hará uso de la entrevista dirigida para conocer la opinión de algunas organizaciones y expertos sobre la necesidad de tener un marco de trabajo para implementar modelos de madurez de seguridad de la información.

La otra fase en la investigación es la comparativa sobre los diferentes modelos existentes y obtener las etapas o pasos que son cruciales para la realización de un marco de trabajo, comparar conceptos y procesos de tal manera que se pueda proponer los pasos más sencillos y prácticos en

[3] Se plantea como un concepto que adquiere significado cuando un signo (palabra) puede provocar la respuesta que está asociada al objeto que representa, Creado por Charles Osgood, George Suci y Persi Tannenbaum, 1957.

su asimilación y facilidad de implementación. La siguiente fase es la analítica para determinar el o los eventos a modificar y los procesos que deben permanecer de acuerdo a las característica esenciales que debe poseer el marco de trabajo. Para estas fases se ejecutará la recolección y análisis de los datos, sabiendo que estas actividades se realizarán en paralelo, se hará uso de la observación, se deberá observar y anotar todo lo que se considere pertinente y el formato puede ser tan simple como una hoja dividida en dos, un lado donde se registran las anotaciones descriptivas de la observación y otra las interpretativas (Cuevas, 2009) y la entrevista esta se define como una reunión para conversar e intercambiar información entre una persona (el entrevistador) y otra (el entrevistado) u otras (entrevistados). El análisis cualitativo implica organizar los datos recogidos, transcribirlos a texto cuando resulta necesario y codificarlos. La codificación tiene dos planos o niveles. Del primero, se generan unidades de significado y categorías. Del segundo, emergen temas y relaciones entre conceptos. Al final se produce teoría enraizada en los datos como resultado de esto se hará un análisis final. Para una mejor comprensión del análisis (Creswell, 1998) simboliza el desarrollo del análisis cualitativo como una espiral, en la cual se cubren varias facetas o diversos ángulos del mismo fenómeno de estudio. Esto se muestra en la figura 23.

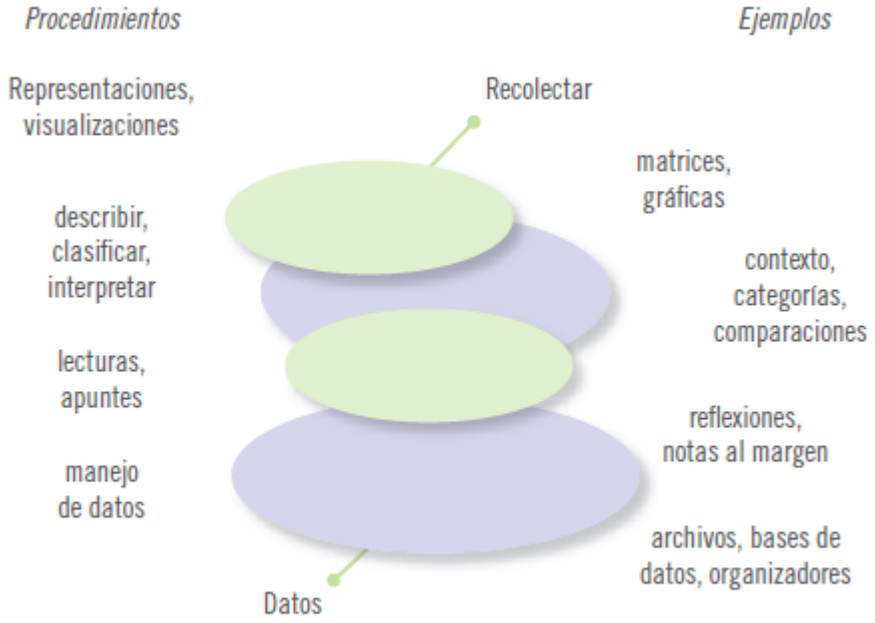


Figura 23. Espiral de análisis de los datos cualitativos.

El paso a seguir es la fase explicativa donde se centrará el o los eventos a modificar, en la fase predictiva se mostraran las posibles dificultades y limitaciones del marco de trabajo para tener claridad si es factible su implementación. Posteriormente, la fase proyectiva se propondrá el diseño dando a conocer como se opera el marco de trabajo de acuerdo a los eventos necesarios y la elaboración del marco de trabajo completo. Por último punto es la fase confirmatoria donde

se analizará y concluyera con el diseño como propuesta final y pasos importantes para la ejecución del diseño.

3.3 Población y Muestra

La población de estudio será empresas que posean una unidad organizacional sobre Seguridad de la Información, Auditoría de Sistemas o Tecnología de la Información donde tengan dentro de sus políticas o procesos la seguridad o alguna persona que dentro de la organización tenga el rol de experto en el tema de seguridad de la información o encargado que posea conocimientos sólidos de este tema, sin importar el rubro de la organización.

El tipo de muestra que se utilizará es la muestra de casos-tipo y muestras homogéneas, la primera donde el objetivo es la riqueza, profundidad y calidad de la información, no la cantidad ni la estandarización. La segunda su propósito es centrarse en el tema a investigar o resaltar situaciones, procesos o episodios en un grupo social. En general el tipo de muestra es dirigida o no probabilística.

En esta fase se determinará el rango de la investigación según el tipo de estudio que es un estudio de caso-tipo será de uno a varios casos de acuerdo al tamaño de muestreo sugerido, para efecto de tener una muestra representativa se realizará una cantidad mínima de 5 empresas. Sin embargo, es de mencionar que el tamaño de la muestra para una investigación con enfoque cualitativo no es importante. Debe tomarse en cuenta que las muestras cualitativas no deben representar a una población (Daymon, 2010), ya que se considera que los casos deben proporcionar un sentido de comprensión profunda del ambiente y problema de estudio.

Las empresas donde se realizarán las entrevistas para obtener la confiabilidad y valoración de la investigación, corresponderán a diversos sectores, tales como: aviación, banca, gobierno, ONG, servicios y financiera.

3.4 Técnicas e Instrumentos de Recolección de Datos

El objetivo de establecer las técnicas e instrumentos de recolección de datos es seleccionar el ambiente que ayude a entender con mayor profundidad un fenómeno del estudio. Para ello es necesario establecer un conjunto de técnicas que nos permitan realizar la recolección de datos adecuado para su posterior análisis. La técnica a emplear para la recolección de datos será de la entrevista dirigida semi estandarizada individual, es dirigida a una población de manera específica como son actores sobre seguridad de la información o que poseen una relación al respecto, es semi estandarizada porque facilitará el enfoque cualitativo, esta consistirá en el empleo de una guía semi estructurada consistente de preguntas que el entrevistador se propone indagar, permitiendo una mayor flexibilidad respecto a la manera, el orden y el lenguaje con que se abordaran los puntos o preguntas, considerándose que se logrará mayor riqueza de datos cualitativos, esta contendrá objetivos específicos de la investigación de campo, las entrevistas serán individuales para que haya mayor apertura, un ambiente de confianza, una relación directa

entre el entrevistador y el entrevistado, permitiendo también obtener información acerca de las opiniones, experiencias o vivencias individuales del entrevistado. Otra técnica a emplear será la observación directa dirigida que retroalimentará la información obtenida de manera holística inicialmente hasta llegar a lo particular, la observación investigativa tendrá varios propósitos tales como: explorar el ambiente y contexto donde se emplean la seguridad de la información, comprender los procesos que vinculan la seguridad de acuerdo al entrevistado y su entorno, el periodo de la observación será abierta hasta la finalización de la investigación. Adicionalmente la observación será utilizada para confirmar los datos de primer orden recolectados en las entrevistas. Se establecerá una muestra inicial de un caso, se evaluará si la unidad es apropiada, se evaluara cada unidad de cada recolección de caso de manera particular. La recolección de datos no tendrá como propósito medir variables, lo que se pretenderá es obtener datos que se conviertan en información de manera profunda, y la finalidad es analizar y comprender generando como resultado conocimiento. La recolección se desarrollara en el ambiente natural de las organizaciones, para ello, el investigador recolectará los datos, siendo este un medio de obtención de información.

3.5 Técnicas de Procesamiento y Análisis de Datos

Se considera la estrecha vinculación que existe entre la conformación de la muestra, la recolección de datos y su análisis, los principales métodos para recabar los datos serán la recolección de documentos y materiales, observación y la entrevista. El análisis cualitativo organizará los datos cualitativos, donde se transcribirá el texto necesario de las entrevistas. El análisis cualitativo será iterativo y recurrente, es decir, no será lineal. El muestreo, recolección y análisis serán actividades casi en paralelo. Conforme avance la inducción de la muestra inicial se generará elementos y unidades que deben analizarse. Siendo este iterativo esto llevará a regresar al campo por más datos enfocados si fuese requerido. En cuanto el análisis detallado el procedimiento a utilizar para el análisis de los datos será la teoría fundamentada, lo cual significa que los hallazgos van emergiendo fundamentados en los datos conforme se van realizando las entrevistas y se van identificando estos hallazgos que sean comunes entre ellas. Se pretende establecer categorías, entiéndase por esto, como conceptos, experiencias, ideas, hechos relevantes y con significado. Se realizará una revisión de los datos de las entrevistas y observación para explorar el sentido general de los datos en su forma original, descubrir las unidades de análisis, generando las explicaciones que fundamentan la propuesta del marco de trabajo.

CAPITULO 4: Propuesta de Diseño del Marco de Trabajo

Para poder desarrollar la propuesta del marco de trabajo se realizó una investigación cualitativa de diferentes modelos existentes, primero se realizó una tabla resumen de los modelos (ver tabla 17), cuyo objetivo era conocer a nivel general cada uno de los marcos de trabajo, programas o modelos revisados, especificando objetivos, características claves y ventajas o beneficios para poder realizar un análisis comparativo, a continuación se muestra la tabla 17:

Componente	FrameWorks				
	ISO/IEC 21827:2002	**PRISMA**	**COBIT Process Assesment Model**	**ISM3**	**IS2ME**
Objetivos	Mejorar y evaluar la capacidad de ingeniería de seguridad	Identificar información sobre deficiencias de los programas de seguridad	Definir el conjunto mínimo de requisitos para llevar a cabo una evaluación que asegure que los resultados son consistentes, repetibles y representativos de los procesos evaluados	Reducir la brecha entre la capacidad SGSI según se define en ISO 27001, el catálogo de los controles de las mejores prácticas identificadas en ISO27002 y la necesidad de que el personal de gestión de seguridad de la información tienen para mejorar continuamente su gestión de la seguridad interna utilizando métricas y modelos de madurez	Disminuir de forma rápida el riesgo asumido por la organización en lo que respecta a seguridad de la información. Esto a través del establecimiento de un marco de implantación de las medidas técnicas y organizativas necesarias
	Aumentar la comprensión de los riesgos de seguridad asociados con una organización	Establecer una línea de base del programa de seguridad para medir la mejora futura siguiendo personal clave o cambios organizativos	Definir la capacidad del proceso en dos dimensiones, capacidad y proceso	Permitir a las organizaciones a identificar y alcanzar los niveles de gestión de seguridad de información adecuada a su industria, perfil de riesgo y a su tamaño	Incorporar la seguridad de la información en la cultura de la organizacional
	Establecer un mecanismo estándar para los clientes para evaluar la capacidad de	Validar la finalización de las acciones correctivas o la postura de	Utiliza indicadores de capacidad de procesos y rendimiento de los procesos para determinar si los atributos de	Proporcionar a las organizaciones oportunidades de certificación, de manera que	Identificar el estado actual de la seguridad de la información de la organización, las acciones de mejora y plan de

Componente	FrameWorks				
	ISO/IEC 21827:2002	**PRISMA**	**COBIT Process Assesment Model**	**ISM3**	**IS2ME**
	ingeniería de seguridad	seguridad de la información del programa	proceso se han logrado	las organizaciones que han certificado su programa de gestión de seguridad de la información a un nivel dado de ISM3 pueden ser reconocidos por su programa de madurez y por lo tanto pueden proporcionar un cierto nivel de fiabilidad independiente a sus clientes en cuanto a la rigurosidad con la que se trata la seguridad de la información	acción para implementación de estas acciones
	Gestionar el grado de confianza en que las necesidades de seguridad se satisfacen	Proporcionar información de apoyo para la tabla de puntuación de la Gestión de la Seguridad de la información Federal (FISMA) e informar	Medir el rendimiento del proceso a través de un conjunto de prácticas base y actividades necesarias para cumplir con los resultados del proceso, así como entradas y salidas de los productos de trabajo asociados a cada proceso	Proporcionar las bases para un ecosistema de la industria para desarrollar todo el área de gestión de seguridad de la información, incluso para formadores en metodología ISM3, la certificación de las implementaciones y profesionales ISM3 y posiblemente, para los	Proponer un método claro y definido de acercamiento de las pequeñas y medianas empresas al cumplimiento de los estándares deseados

Componente	FrameWorks				
	ISO/IEC 21827:2002	**PRISMA**	**COBIT Process Assesment Model**	**ISM3**	**IS2ME**
				proveedores de software de información herramientas de gestión de la seguridad	
	Establecer el Nivel de Capacidad sobre la madurez de las organizaciones de ingeniería de seguridad.	Preparar a favor o efectuar una estimación, evaluación o una revisión de un programa de seguridad de la información	Medir la capacidad de los procesos por el logro del atributo (escala) a través de la evidencia especifica (nivel 1) y genérica (nivel superior) de las prácticas y productos de trabajo		Sentar las bases para posterior desarrollo en profundidad hacia el cumplimiento e implantación total del SGSI según las normas existentes, si así se requiere
	Monitorear la postura de Seguridad en la Organización		Ser un motor fuerte y eficaz para la mejora de procesos		
Características Clave	Es un modelo de referencia de proceso.	Tiene un orden bien establecido para medir la seguridad de la información	Orientado a la evaluación (assessment) de procesos de TI dentro de las organizaciones	Basada en un enfoque completamente en procesos de gestión de la seguridad de la información y madurez, sobre el principio que cada control necesita un proceso para ser manejado	Metodología adaptable a pequeñas y medianas organizaciones y de resultados a corto plazo
	Se centra en la madurez de los procesos	Es preciso para establecer la madurez de la seguridad de la información	El modelo sirve como documento base de referencia para la realización de evaluaciones de la capacidad de los procesos actuales de TI	Rompe la gestión de la seguridad de la información en un amplio pero manejable número de procesos, con controles de seguridad específicamente relevante a	Mitigación del riesgo a corto plazo

Componente	FrameWorks				
	ISO/IEC 21827:2002	**PRISMA**	**COBIT Process Assesment Model**	**ISM3**	**IS2ME**
				ser identificados dentro de cada proceso como un subconjunto principal de ese proceso	
	Se centra en los requisitos para la implementación de la seguridad en un sistema o conjunto de sistemas relacionados	Establece con claridad los roles que intervienen en la evaluación	Provee una metodología comprensible, lógica, repetible, confiable y robusta para evaluar la capacidad de los procesos de TI	Define la madurez de la gestión de la seguridad de la información en términos de la operación de un adecuado y complementario conjunto procesos de seguridad de información ISM3	Gestión de la seguridad de la información de una forma eficiente, eficaz y práctica
	Herramienta para organizaciones de ingeniería para evaluar sus prácticas de ingeniería de seguridad y definir las mejoras	Determina las brechas de los programas de seguridad de la información		Define la Capacidad en términos de métricas y las prácticas de gestión utilizadas	Marco que ayuda a la organización a iniciar la ruta hacia el cumplimiento de los estándares deseados
	Método de las organizaciones de evaluación de la ingeniería de seguridad tales como certificadores y evaluadores pueden establecer la confianza en la capacidad	La forma de obtención de la información cuando se evalúa la seguridad se hace a través de entrevista lo que permite una profundización, valorización de los datos,		Los Niveles de Madurez ayudan a las organizaciones a seleccionar la escala SGSI más apropiada para sus necesidades	

Componente	FrameWorks				
	ISO/IEC 21827:2002	**PRISMA**	**COBIT Process Assesment Model**	**ISM3**	**IS2ME**
	de la organización como una entrada al sistema o la garantía de la seguridad de los productos	garantizando una documentación completa, complementada con la observación			
	Mecanismo estándar para los clientes para evaluar la capacidad de ingeniería de seguridad de un proveedor	identifica y rastrea las influencias y limitaciones ambientales positivas y negativas que influyen en el programa de seguridad de la información		El espectro de la madurez facilita el equilibrio de costos, riesgo, la usabilidad y habilita la mejora incremental, benchmarking y objetivos a largo plazo	
				Ofrece un enfoque a las organizaciones de flexibilidad para seleccionar cualquier subconjunto de procesos de seguridad de la información basado en criterios variados.	
Ventajas o Beneficios	Mejora la calidad	Utiliza niveles de madurez para evaluar	Mejora el rigor y la fiabilidad de las revisiones de los procesos de TI	Amigable con el negocio	Se puede aplicar a pequeñas y medianas organizaciones
	Mejora la disponibilidad	Revisa el nivel de gestión, no específicamente la parte técnica	Mejora los procesos de TI	Adaptable	Versión en español directa de sus autores
	Reduce el costo de	Utiliza la información	Facilita la realización de	Acreditable	Implementación seguridad de la

Componente	FrameWorks				
	ISO/IEC 21827:2002	**PRISMA**	**COBIT Process Assesment Model**	**ISM3**	**IS2ME**
	entrega de sistemas seguros	proporcionada por los propietarios del sistema, con el uso de entrevistas, y el uso de muestras limitadas para efecto de tener información de confianza	Auditorías o Evaluaciones de la capacidad de los procesos específicos de TI		información a corto plazo y con utilización razonable de recursos
	Productos de confianza	Proporciona un metodología para la realización de un revisión	Ofrece esta consistencia y confiabilidad para que los líderes de negocio y de TI puedan confiar en el proceso de evaluación y en la calidad de los resultados mientras maximizan el valor del negocio de sus inversiones en TI	Fácil de implementar	
	Servicios de ingeniería de seguridad	Utiliza los niveles de madurez basados en CMM		Compatible	
	Utiliza los niveles de madurez basados en CMM	Proporciona una metodología para la realización de una revisión de la seguridad de manera clara y concreta		Escalable y Completa	
		Permite la certificación y acreditación del		Abierto	

Componente	FrameWorks				
	ISO/IEC 21827:2002	**PRISMA**	**COBIT Process Assesment Model**	**ISM3**	**IS2ME**
		programa			
				Basada en procesos	
				Uso de métricas	

Tabla 17. Vistazo general de marcos de trabajo.

Una vez conociendo las características y ventajas de cada modelo, se procedió a determinar ciertos criterios que nos permitieran conocer más los modelos de madurez investigados, para ello se utilizó la siguiente tabla comparativa (ver tabla 18), cuyo objetivo fue analizar mediante un listado de criterios los marcos de trabajo investigados, para poder determinar factores importantes que deben ser retomados o mejorados en la propuesta. La fuente principal de donde los criterios fueron seleccionados está basada en el análisis de cada marco y sus aportes.

CRITERIO	FRAME WORK				
	ISO/IEC 21827:2002	PRISMA	COBIT Process Assesment Model	ISM3	IS2ME
Tipo de Organización	Todo tipo	Todo tipo	Todo tipo	Todo tipo	Todo tipo
Tamaño de Organización	Todo tamaño	Todo tamaño	Todo tamaño	Pequeñas y Grandes Organizaciones	Pequeña y Mediana Organizaciones
Alcance	Implementación de seguridad en un Sistema de Software	Revisión Madurez de programas de seguridad	Evaluación de Procesos de TI	Implementar SGSI	Bases para implementar SGSI
Enfoque	Procesos de los Sistemas	Holístico	Procesos de TI	Holístico	Holístico
Orientación	Procesos	Áreas	Procesos	Procesos	Fases Secuenciales
Alineamiento de seguridad a los objetivos del negocio	Toma en cuenta objetivos del negocio	Ayuda a reducir la interrupción de las operaciones y los activos críticos	La capacidad de los procesos de TI para cumplir los objetivos del negocio	Alinea la gestión de la seguridad con las necesidades del negocio	Al presentar y gestionar autorización de la alta dirección se ajusta y modifica tomando en cuenta estrategias globales de negocio
Ayuda a cumplir requerimiento de regulaciones	No especifica	Debe ser considerado	Considera dentro de sus procesos uno que vele por el cumplimento de las leyes, regulaciones y contratos	Se implementa de acuerdo a la regulación aplicable	Enumeración y descripción regulaciones que la organización debe cumplir
Auto Aplicado	Se requiere consultor	Se requiere consultor	Se requiere consultor	Cuenta con guía de implementación, es posible después de un profundo estudio implementarlo	No específica, pero se considera un marco de apoyo
Flexibilidad	Flexible	Rígido	Flexible	Permite implementarlo de acuerdo a contexto y uno de sus beneficios es la fácil	Flexible y Adaptable

CRITERIO	FRAME WORK				
	ISO/IEC 21827:2002	PRISMA	COBIT Process Assesment Model	ISM3	IS2ME
				implementación	
Crea Valor	Confianza y Eficiencia	Facilita la Acreditación generándole credibilidad y confianza en sus procesos.	provee una metodología comprensible, lógica, repetible, confiable y robusta para evaluar la capacidad de los procesos de TI	Permite a las organizaciones identificar y alcanzar niveles de gestión de seguridad de información adecuada al contexto de cada organización	Reducción de riesgo haciéndola más rentable
Identifica y Evalúa Riesgos	Una de sus principales áreas es la evaluación de riesgos como parte de la gestión de seguridad. Evalúa y Cuantifica el riesgo.	Es un enfoque basado en el riesgo. Posee un marco de trabajo de gestión del Riesgo donde categoriza la información, seleccionar los controles de seguridad, evalúa y monitorea el riesgo constantemente.	Los valores derivados de las evaluaciones que utilizan este modelo incluyen resultados fiables que centran a la empresa sobre los riesgos, beneficios y consecuencias financieras derivadas del rendimiento y la capacidad de sus procesos de TI	ISM3 cubre la actividad de gestión de evaluación de riesgos	Identifica y Evalúa

Tabla 18. Análisis de Criterios en los marcos de referencia.

En base a la información recopilada y el análisis comparativo realizado se determinó un listado de las fases que plantea cada modelo y se desarrolló la siguiente tabla comparativa (ver tabla 19).

		ISO21827	PRISMA	COBIT	IS2ME	ISM3
1	Entender el Problema	x		x		
1	Evaluar la Seguridad				x	
2	Determinar o definir las necesidades (requerimientos)	x	x			
2	Determinar Alcance		x	x		
2.5	Establecer Objetivos del Estudio / Proyecto					x
2.5	Presentar los objetivos a los Interesados		x			
2.5	Determinar la meta de madurez					x
3	Planificar los recursos del Proyecto		x			
3	Nombrar un CISO, Conformar Comité Ejecutivo de Seguridad y el Comité de Seguridad de la Información					x
3	Nombrar un Asesor o Equipo Externo		x	x		
3	Establecer interlocutores o Equipo o Comité Interno				x	x
4	Aprobación de Dirección Corporativa de evaluación de seguridad				x	
4	Establecer las restricciones y criterios de competencia			x		
4	Determinar requerimientos regulatorios y adicionales					x
5	Evaluación de seguridad				x	
5	Fase de Revisión		x			
5	Proceso de evaluación,			x		
5	Evaluación de SGSI Actual a SGSI basado en ISM3					
5	Evaluar Seguridad	x				
5.1	Planeación			x		
5.2	Recolección de Datos		x	x		
5.2	Recolección General de Información / Recolección Técnica Info				x	
5.2	Desarrollar Entrevista		x			
5.3	Análisis de Información		x		x	
5.3	Validación de Datos			x		
6	Informe de Estado de Seguridad				x	
6	Presentación de informes, Realizar reporte		x	x		

		ISO21827	PRISMA	COBIT	IS2ME	ISM3
7	Análisis de Brecha de SGSI Actual a SGSI basado en ISM3					x
7	Desarrollo y Presentación de Documento Plan de Acción de Seguridad y Protección de la Información				x	
7	Retroalimentación	x	x			
	Verificar los resultados					

Tabla 19. Tabla comparativa de las diferentes fases que se encuentran en los modelos de madurez investigados.

Con toda esta información a continuación se presenta el diseño de un marco de trabajo para la implementación de un modelo de madurez de seguridad de la información, este modelo será adaptable a cualquier organización, sin importar su tamaño en cuanto a personal o capital. El modelo está comprendido por las siguientes fases (Figura 24):

Figura 24. Fases del modelo de madurez de la seguridad de la información propuesto

El modelo propuesto está conformado por ocho fases, las cuales se describen a continuación:

4.1 Fase I Contextualizar la Seguridad de la Información en la Organización

Figura 25. Fase I Contextualizar la seguridad de la información en la organización

Esta fase permitirá establecer el contexto interno y externo referente a la seguridad de la información en la organización, identificando un panorama general de la organización de todo aquello que influencie o afecte a la seguridad de la información. Además se establecerá el fundamento o la necesidad de realizar la medición de la madurez de la Seguridad de la Información. Adicionalmente, la necesidad de la evaluación variará de forma única en la organización ya sea en un contexto interno o externo. Posteriormente, se deberá analizar los objetivos del negocio dentro del contexto de la organización, en esta parte se debe tener claridad que se entiende por contexto interno y externo.

- **Contexto Interno:** Políticas, objetivos de la organización, cultura de la organización, estructura organizacional, normativas, guías, modelos, recursos y riesgos.
- **Contexto Externo**: Cultural, regulatorio y tecnológico.

Posteriormente se debe determinar la situación actual de la organización, en ella se debe contemplar cuales son los procesos o medidas que se realizan en la organización que afectan a la seguridad de la información.

En caso la organización no cuente con una evaluación de riesgos se recomienda hacer el estudio sobre los riesgos de la organización. Se debe entender por evaluación de riesgos como el proceso de identificación de los problemas que todavía no han ocurrido. Los riesgos se evalúan mediante el examen de la probabilidad de la amenaza y la vulnerabilidad y considerando el impacto potencial de un incidente no deseado. Asociado con esa probabilidad es un factor de incertidumbre, que variará dependiendo de una situación particular. Esto significa que la probabilidad sólo se puede predecir dentro de ciertos límites. Además, el impacto evaluado para un riesgo en particular también está asociado la incertidumbre, ya que el incidente no deseado puede no resultar como se esperaba. Debido a que los factores pueden tener una gran cantidad de incertidumbre en cuanto a la exactitud de las predicciones asociadas a ellos, la planificación y la justificación de la seguridad puede ser muy difícil. Una forma de abordar parcialmente con este problema de una manera costo-efectiva es la implementación de técnicas para detectar la ocurrencia de un incidente no deseado.

Un incidente no deseado se compone de tres componentes: amenaza, vulnerabilidad e impacto. Las vulnerabilidades son propiedad de los activos que pueden ser explotadas por una

amenaza, e incluyen debilidades. Si bien la amenaza o la vulnerabilidad no están presentes, no puede haber ningún incidente no deseado y por lo tanto no hay riesgo. La gestión de riesgos es el proceso de evaluar y cuantificar los riesgos y el establecimiento de un nivel aceptable de riesgo para la organización. La gestión de riesgos es una parte importante de la gestión de la seguridad y para esta fase es clave para tener una mayor precisión al realizar una medición de la seguridad de la información de la organización.

Como resultado de esta fase se debe obtener un autodiagnóstico, la evaluación de riesgos, Objetivos Estratégicos de Seguridad de la Información basado en el contexto de la organización, la vinculación de objetivos de negocio a los objetivos de TI y la vinculación de los objetivos de TI a los procesos de TI.

4.2 Fase II Definir el Alcance

Figura 26. Fase II Definir el Alcance

En esta fase se define el alcance de la evaluación de la seguridad de la información, de acuerdo al ámbito del desarrollo de la evaluación basado en las necesidades que se establecieron en la fase previa, se establecen los resultados que se esperan de la evaluación esto se realiza en cuatro subfases que buscan definir claramente el alcance tales como: *establecer los objetivos de la evaluación, determinar las metas de madurez, determinar requerimientos y restricciones, solicitar autorización de la alta dirección*. Adicionalmente, un aspecto que puede ser de mucho utilidad en la definición del alcance es establecer los límites de lo que debe contener la evaluación así como lo que no va a contener, esto permitirá tener una mejor claridad a los interesados de los resultados esperados.

4.2.1 Establecer los objetivos de la evaluación

Se debe determinar lo que la organización necesita alcanzar, en base a sus objetivos del negocio, con la implementación de un modelo de madurez de la seguridad de la información, estos deben ser claros porque serán la guía a seguir durante la evaluación. El establecimiento de los objetivos de seguridad y las metas de seguridad requieren realizar un análisis de dependencias para poder operacionalizar los objetivos identificados para la evaluación.

Definiciones operacionales

No se pretende medir la naturaleza del objetivo sino describir cómo se mide, logrando una definición particular del observador. El observador obtiene la misma medida y es repetible. Los beneficios de la utilización de unidades son que facilita su gestión y comunicación. El marco de trabajo instituye operacionalizar los objetivos previos a objetivos de seguridad de la información. Para realizar las definiciones operacionales es necesario realizar preguntas como las siguientes:

Políticas de Seguridad de la Información
¿Cuenta con políticas de seguridad? Cuenta con una política para el uso de correo electrónico? ¿Se han identificado los sistemas que contienen datos críticos? ¿Se cuenta con la documentación de los sistemas y los datos que se manejan?
Como la seguridad de la información es organizada
¿Se cuenta con una estructura organizativa dedicada propiamente a la Seguridad de la Información? ¿Cada cuánto se evalúan las funciones de cada uno de los miembros del equipo de Seguridad de la información?
Seguridad de Recursos Humanos
¿Cuántas revisiones de antecedentes pasan en el año? ¿Con cuánto tiempo de anticipación RRHH solicita la desactivación de los usuarios que se retiran? ¿Notifica RRHH a TI cuando los usuarios se van a retirar?
Gestión de Activos
¿Cuántos inventarios de activos se realizan al año? ¿Se cuenta con un listado de activos críticos?
Control de Acceso y Manejo Acceso de Usuario
¿Quiénes son los usuarios de los servicios? ¿Se requiere autorización específica? ¿Se cuenta con procedimientos establecidos para verificar el control de acceso? ¿Se cuenta con una política de seguridad que abarque el control de acceso?
Tecnología Criptográfica
¿Es cifrada la información sensitiva? ¿Se utilizan certificados de seguridad

Seguridad Física de los Sitios y Equipos de la Organización
¿Se cuenta con un historial de bitácoras de acceso al data center? ¿Qué personas tienen acceso a los servidores?
Seguridad Operacional
¿Cuántas interrupciones son aceptables? ¿Se realizan pruebas de restauración de respaldos periódicamente? ¿Existe revisión de logs de manera periódica? ¿Cuál es el número máximo de transacciones que se pueden perder debido a una interrupción?
Comunicaciones y Transferencia de Datos Seguros
¿Las redes se encuentran segmentadas? ¿La transferencia de información entre dos partes es asegurada?
Adquisición, desarrollo y soporte de sistemas de información seguros
¿Se realiza una evaluación de seguridad a los sistemas de información antes de lanzarlos a producción? ¿Se aplican buenas prácticas de aseguramiento al diseño y desarrollo de sistemas?
Seguridad para proveedores y terceros
¿Los proveedores o terceros conocen las políticas de seguridad de la organización? ¿Los proveedores y terceros cuentan con buenas prácticas de seguridad de la información?
Gestión de incidentes de seguridad de la información
¿Existe un proceso documentado para el manejo de incidentes? ¿Los empleados han recibido capacitación sobre el proceso de manejo de incidentes?
Gestión de Continuidad del Negocio
¿Existe un plan de contingencia y recuperación de desastres? ¿Cada cuánto se realiza la verificación de los planes de contingencia y recuperación de desastres? ¿Cuándo fue la última vez que se actualizó el plan de contingencia y recuperación de desastres?
Cumplimiento
¿El sistema maneja información personal de clientes, clientes potenciales, interesados o empleados? ¿Cuáles regulaciones aplican a la organización?

4.2.2 Determinar las metas de la madurez

Se debe describir concretamente que se realizará con la implementación del modelo de madurez de seguridad de la información. Al establecer las metas de seguridad se deberá entender la desviación máxima del resultado deseado que la organización tolera antes de tomar una acción correctiva. Las metas de seguridad son normalmente definidas en términos de frecuencia de ocurrencia y límite de costo. Las metas de seguridad muestran lo que la organización espera para su información.

4.2.3 Determinar requerimientos y restricciones

Algo vital al realizar una evaluación de madurez es plantear los requerimientos que la organización busca alcanzar. Además de establecer las restricciones que se deben considerar, políticas, normas, regulaciones entre otros, para ello, se debe tomar en cuenta las siguientes restricciones:

- ¿Es una "instantánea en el tiempo" y sólo tiene en cuenta los datos históricos y los datos disponibles en el momento en que la revisión se lleva a cabo?
- ¿Es subjetiva utilizando una metodología definida y asume que todos los datos de la entrevista son válidos y correctos?
- Es ejecutado por individuos con conocimientos de Seguridad, estándares internacionales como ISO de la familia 27000, asesoría y programas de seguridad.
- Es un proceso estandarizado o no estructurado para la recolección y la calificación de la información, pero requiere de un análisis por miembros del equipo.
- La revisión ayudará a la certificación y acreditación (C & A) del dominio o proceso, se centra en el marco, modelo o programa de seguridad.

4.2.4 Solicitar Autorización a la Alta Dirección

Se debe preparar una presentación donde se busque la autorización de la definición del alcance por parte de la alta dirección. Esta presentación debe identificar los mensajes claves que se desean transmitir en un lenguaje entendible para este nivel de la organización. Además para poder llevar a cabo la implementación del modelo de madurez es de vital importancia contar con la aprobación de la alta dirección, contar con este apoyo incentiva la colaboración y el involucramiento de todas las áreas de la organización.

4.3 Fase III Establecer Roles Y Responsabilidades

Una parte importante durante la implementación de modelos de madurez es realizar la definición de equipos que permitan realizar el proceso de evaluación, así como determinar las personas involucradas en dicho proceso que formen parte de las áreas clave de evaluación. Debido a esto se ha determinado esta fase.

Figura 27. Fase III Establecer roles y responsabilidades

4.3.1 Conformar Comité Ejecutivo de Seguridad de la Información (Adhoc)

Para poder desarrollar una adecuada implementación de modelos de madurez, se recomienda la conformación del Comité Ejecutivo de Seguridad de la Información (Adhoc), al cual la alta dirección delegue autoridad y responsabilidad para llevar a cabo una implementación adecuada y toma de decisiones oportunas. El comité puede estar conformado por al menos un miembro de la alta dirección y el resto de miembros deben ser de confianza de la alta dirección o personal clave de la seguridad. En caso contrario la persona que tenga conocimientos de seguridad y se le haya delegado supervisar la seguridad de la información dentro de la organización.

4.3.2 Conformar Equipo implementador

El equipo implementador, es un equipo interno o externo, el cual es el encargado de llevar a cabo la implementación de la evaluación a través del modelo de madurez de seguridad de la información.

Equipo Implementador externo

Este equipo está conformado por consultores especializados que conocen el modelo y cuentan con experiencia para implementarlo. Debe poseer conocimiento, habilidades y experiencia con el modelo de referencia de dominios, el modelo de evaluación de dominios, métodos, herramienta, procesos de calificación, conocimiento de los procesos y dominios que van a ser evaluados, atributos personales que contribuyan a una evaluación efectiva.

Equipo Implementador Interno.

En caso la organización decida implementar el modelo por su propia cuenta que cumpla al menos con las siguientes características:

- Contar con un interés personal en el resultado
- Competente
- Motivado
- Empoderado
- Conocer a profundidad el modelo.

4.3.3 Establecer Personal Clave de áreas involucradas

Para poder llevar a cabo una implementación es de suma importancia identificar al personal clave que podrá en un primer momento proporcionar información necesaria de las áreas o procesos a las que se les hará la evaluación y facilite la ejecución de cada una de las fases del modelo.

4.4 Fase IV Planear la Evaluación de la Seguridad de la Información

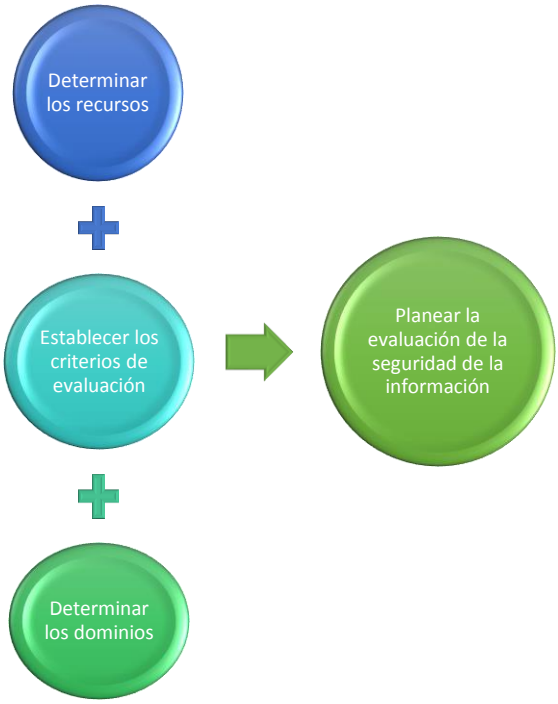


Figura 28. Fase IV Planear la evaluación de la seguridad de la información

La fase de planificación de la evaluación deberá describir todas las actividades que se realizaran en la evaluación, el plan debe ser desarrollado junto con un programa de evaluación, deberá incluir la determinación de recursos, el tiempo estimado de la evaluación, el establecimiento de preguntas para determinar la evidencia de los criterios de evaluación y la selección de los dominios.

Se deben establecer los resultados esperados de la evaluación, que es lo que la parte interesada desea, verificar el cumplimiento de los requisitos. Los posibles factores de riesgo y estrategias de mitigación deberán estar documentados, priorizados y rastreados a través de la planificación de la evaluación. Todos los riesgos identificados se controlarán durante la evaluación. Los riesgos potenciales pueden incluir cambios en el equipo implementador, cambios organizacionales, cambios en el propósito del / alcance / evaluación, la falta de recursos para la evaluación, la confidencialidad, la prioridad de los datos. Se debe determinar el método para recolectar, revisar, evaluar y documentar la información necesaria para la evaluación.

Durante esta fase se debe coordinar con el equipo implementador las actividades de evaluación con la unidad organizativa que está siendo evaluada, se deben cumplir los requisitos de espacio de trabajo, programación, compatibilidad y disponibilidad de las personas claves identificadas.

Revisar y obtener la aceptación del plan por parte del comité ejecutivo. El plan adicionalmente incluye el programa de evaluación y logística de visitas al sitio que debe ser revisado y aprobado. Obtener la Confirmación del compromiso de la parte interesada para proceder con la evaluación.

4.4.1 Determinar los recursos (financiero, tecnológico, humano)

Para una adecuada evaluación es importante determinar los recursos necesarios para llevar a cabo la evaluación de la seguridad, entre los cuales puede contarse con recursos financieros, tecnológicos y de personal. Se deberá establecer un calendario de planeación del tiempo estimado para asegurar los recursos necesarios durante el periodo de la evaluación, para esto se propone el uso de una matriz de recursos.

4.4.2 Establecer los criterios de evaluación

Para cada dominio evaluado, se debe determinar un nivel de madurez, para ello se utiliza un conjunto definido de criterios de evaluación en el modelo de madurez. La trazabilidad debe mantenerse entre la evidencia objetiva recogida y los niveles atribuidos al dominio. Para cada proceso de clasificación, la relación entre los criterios y las pruebas objetivas deben registrarse.

Se debe determinar el método para recolectar, evaluar, revisar y documentar la información necesaria para la evaluación, para ello se debe establecer la estrategia y las técnicas para la selección, recopilación, el análisis de los datos y la justificación del nivel de madurez establecido debe identificarse explícitamente y ser demostrable.

Criterios y Niveles de Madurez

Para poder realizar la evaluación, una vez seleccionados los dominios, se procede a utilizar las cuatro tablas de evidencia de nivel de madurez, una por cada criterio de evaluación que plantea el modelo. En cada tabla se encuentra los cinco niveles de madurez que define el modelo por cada criterio y las posibles evidencias por nivel de madurez que se deben encontrar para poder valorar el dominio en el nivel de madurez que le corresponde, al momento de realizar la evaluación, esto puede realizarse a través de una entrevista, cuestionario u otro instrumento. Queda a libre selección del evaluador el instrumento a utilizar.

Para el registro de la evidencia o los hallazgos, el evaluador puede auxiliarse de la *tabla de registro.* El uso de la tabla consiste en escribir la evidencia encontrada al momento de realizar entrevistas, cuestionarios u otro.

Dominio	**Criterio**				
	Iniciado	**Básico**	**Establecido**	**Gestionado**	**Optimizado**
Dominio 1	No se encontró				
Dominio 2		Propuesta presentada a la gerencia			

Tabla 20. Registro Ejemplo

La *tabla de registro* (Ver Tabla 20) tiene por objetivo registrar o documentar con evidencia el nivel de madurez que cada dominio tiene desde la perspectiva de cada criterio.

Antes de detallar las tablas de registro, es importante conocer cada criterio.

Criterios

El modelo de evaluación define cuatro criterios de evaluación de madurez para cada dominio seleccionado.

En términos generales el objetivo de los criterios es medir la madurez de cada dominio en cuatro dimensiones diferentes y de esta forma la organización tenga una evaluación de su seguridad de la información desde cuatro dimensiones o perspectivas diferentes. El modelo está abierto a que la organización utilice otros criterios que considere pertinentes para una evaluación de seguridad, en este caso únicamente se debe retomar la metodología que plantea para uso de criterios.

Gestión Documental

La documentación de los dominios es un criterio de madurez, en el cual puede evaluarse la evolución de documentación de cada dominio. Los dominios pueden existir pero en algunos casos pueden no estar documentados.

Dominio	**Gestión Documental**				
	Iniciado	**Básico**	**Establecido**	**Gestionado**	**Optimizado**
Dominio 1					
Dominio 2					
Dominio N					

Tabla 21.Registro de Gestión Documental

Automatización

La automatización de los procesos es una forma de medir la madurez de los dominios, en este sentido un dominio cuando sus procesos son manuales puede considerarse que tiene cierta falta de madurez, mientras en la medida que sus procesos son automatizados se puede observar el progreso de su madurez. Considerando que al tener automatizado el dominio puede existir un mejor control , trazabilidad y precisión Ver Tabla 22.

Dominio	**Automatización**				
	Iniciado	**Básico**	**Establecido**	**Gestionado**	**Optimizado**
Dominio 1					
Dominio 2					
Dominio N					

Tabla 22.Registro de Automatización

Aseguramiento

El criterio de Aseguramiento es fundamental debido a que evalúa el nivel en que un dominio está siendo revisado y auditado con el fin de asegurar los requerimientos mínimos y también es una entrada para que los procesos de un dominio sean madurados. Ver Tabla 23.

Dominio	Aseguramiento				
	Iniciado	Básico	Establecido	Gestionado	Optimizado
Dominio 1					
Dominio 2					
Dominio N					

Tabla 23. Registro de Aseguramiento

Medible

Existe un principio para la mejora como lo menciona David Herce "lo que no se mide no se mejora", en un proceso de madurez este criterio es importante porque evalúa si el dominio está siendo medido y con qué profundidad. Ver Tabla 24.

Dominio	Medible				
	Iniciado	Básico	Establecido	Gestionado	Optimizado
Dominio 1					
Dominio 2					
Dominio N					

Tabla 24.Registro de Medible

Niveles de Madurez

Como se mencionó anteriormente, el modelo define cinco niveles de madurez:

- Iniciado
- Básico
- Establecido
- Gestionado
- Optimizado

Con estos la organización puede evidenciar el nivel de madurez que se encuentra cada dominio evaluado.

La metodología para hacerlo es mediante el uso de cuatro tablas de evidencia de nivel de madurez, las cuales se detallan a continuación (Ver Tablas 25, 26, 27 y 28):

Nivel de Madurez		Criterio
		Gestión Documental
1	**Iniciado**	La organización no posee documentación del dominio. La documentación está a nivel de ideas generales o esbozos. Durante el proceso no se registra documentación. La documentación es adhoc y desorganizada. La documentación surge de manera reactiva.
2	**Básico**	La organización posee propuestas presentadas a cualquier nivel jerárquico. La documentación está estructurada y con ideas concretas. Durante el proceso del dominio se registra información básica. La documentación sigue un estándar de la organización. La organización dispone de prácticas de documentación.
3	**Establecido**	La organización posee documentación del dominio a nivel de desarrollo, borradores o preliminar después de que la propuestas han sido autorizadas.

Nivel de Madurez		Criterio
		Gestión Documental
		La documentación adicionalmente a estar estructurada, ha pasado por procesos de revisiones. Durante el proceso del dominio se registra información siguiendo estándares. La documentación sigue un estándar mejorado. La organización dispone de prácticas de documentación mejoradas. La documentación se encuentra pero desactualizada.
4	**Gestionado**	La organización posee documentación completa del dominio. La documentación posee un sistema de gestión documental dentro de la organización. La documentación se mantiene actualizada.
5	**Optimizado**	La gestión documental se auxilia de software para optimizar todos los procesos de documentación. La documentación adopta estándares de externos o de calidad para su gestión. La documentación se gestiona aplicando controles de seguridad.

Tabla 25. Evidencia de Nivel de Madurez - Gestión Documental

Nivel de Madurez		Criterio
		Automatización
1	**Iniciado**	Los procesos del dominio son manuales. Existe cierta automatización adhoc. Algún proceso del dominio puede ser automatizado de manera reactiva.
2	**Básico**	Se ha logrado automatizar alguna parte de los procesos. Existen propuestas formales de automatización de procesos del dominio. Existen procesos automatizados con errores o deficiencias. Se apoya de herramientas para facilitar los procesos.
3	**Establecido**	Los procesos críticos del dominio son automatizados. Los procesos del dominio están siendo automatizados completamente. Deficiencias en la automatización están siendo superadas. La organización dispone de buenas prácticas de automatización.
4	**Gestionado**	Los procesos del dominio son automatizados. La automatización de procesos del dominio es gestionada adecuadamente por un área delegada. La automatización es monitoreada periódicamente. Los procesos automatizados del dominio se mantienen actualizados. Se dispone de sistemas de información que soportan los procesos.
5	**Optimizado**	Los procesos automatizados del dominio sufren actualizaciones periódicas y programadas. Los sistemas de información son actualizados e incorporan nuevas características. Se adoptan estándares externos de calidad y otros para los procesos automatizados. Todos los procesos automatizados se les aplican controles de seguridad.

Tabla 26. Evidencia de Nivel de Madurez - Automatización

Nivel de Madurez		Criterio
		Aseguramiento
1	**Iniciado**	Inexistencia de revisiones internas. Inexistencia de auditorías. Revisiones y/o auditorias adhoc.

Nivel de Madurez		Criterio
		Aseguramiento
		Revisiones y/o auditorias reactivas.
2	**Básico**	Revisiones internas básicas. Existes practica institucionales de revisión y auditorías. La organización cuenta con monitoreo o supervisión de áreas críticas.
3	**Establecido**	Los diferentes niveles de mando de la organización cuentan con programa estructurado de revisión de los procesos del dominio. Se tiene definido niveles de cumplimiento los cuales son revisados y auditados. La organización.
4	**Gestionado**	Existen planes de acción cuando se tienen deficiencias en los controles implementados. El departamento de auditoria interna cuenta con personal capacitado en cada dominio. Existe unidad o personal de cumplimiento. Existe un programa interno periódico de auditorías.
5	**Optimizado**	Existe al menos una vez al año auditorías externas. La organización invierte recursos para superar las no conformidades. Está conformado el departamento de Control Interno.

Tabla 27. Evidencia de Nivel de Madurez - Aseguramiento

Nivel de Madurez		Criterio
		Medible
1	**Iniciado**	La organización carece de métricas. Existen métricas adhoc.
2	**Básico**	Los procesos del dominio cuentan con métricas básicas. Existen propuestas formales de definición de métricas. Existen ciertos patrones establecidos para la definición de métricas.
3	**Establecido**	Métricas establecidas con objetivos claramente definidos. Proceso de adopción de métricas para las diferentes áreas de la organización.
4	**Gestionado**	Establecimiento de sistema de métricas para cada dominio Implementación de técnicas como Balance Scorecards. La organización está comprometida a dar cumplimiento a sus métricas con sus indicadores.
5	**Optimizado**	Adopción de diferentes técnicas de medición Prácticas de mejora de métricas. Incorporación de herramientas de software para facilitación del sistema de métricas.

Tabla 28. Evidencia de Nivel de Madurez - Medible

Con el listado de posibles evidencias, el evaluador tiene certeza que debe buscar para poder colocar al dominio el nivel de madurez que le corresponde de acuerdo a criterio medido.

4.4.3 Determinar los dominios

Para este modelo de seguridad se proponen dominios, los cuales permitirán realizar una radiografía de la situación en la que se encuentra la Organización con respecto a la Seguridad de la Información.

El modelo de evaluación de madurez del marco de trabajo está compuesto por la combinación de diferentes compontes que al adoptarlos es posible evaluar la madurez de la seguridad de la información de la organización. Entre los componentes se tienen:

- Dominios: Áreas relacionadas con seguridad de la información dentro de una organización.
- Criterios: Elementos para evaluar la madurez de los dominios.
- Niveles de Madurez: Niveles de avance o mejora para poder medir la madurez de un dominio en el momento de la evaluación, plantearse un nivel deseable y en una siguiente evaluación observar su progreso. Los niveles de madurez ayudaran al evaluador a determinar el nivel de madurez del dominio en base a la evidencia encontrada.

Dominios

Lo primero es establecer los dominios que van a ser evaluados de la organización, basados en las fases "Contextualizar la Seguridad de la Información en la Organización" y "Definir el Alcance", la cual incluye un análisis y evaluación de riesgos. El modelo retoma los dominios que establece la ISO/IEC 27001:2013 (ISO/IEC, 2013), debido a que por ser un estándar internacional de seguridad de la información ofrece una completa cobertura de todas las áreas que componen la seguridad de la información dentro de una organización, además de los dominios de la ISO, se ha incluido uno adicional, el cual se considera fundamental para gestión de la seguridad de la información dentro de una organización y es el Análisis y Evaluación de Riesgos.

Descripción de Dominios

En la siguiente tabla (Ver tabla 29) se describe brevemente cada dominio.

No.	Dominio	Descripción
1	Análisis y Evaluación de Riesgos	Controles del análisis y evaluación de riesgos en la organización
2	Políticas de Seguridad de la Información	Controles de como las políticas son asignadas y revisadas
3	Como la seguridad de la información es organizada	Controles de como las responsabilidades son asignadas y también incluye los controles para dispositivos móviles y teletrabajo
4	Seguridad de Recursos Humanos	Control prioritarios para empleados durante y después de emplearlo
5	Gestión de Activos	Controles relacionados al inventario de activos y uso aceptable, también para clasificación de información y manejo de medias
6	Control de Acceso y Manejo Acceso de Usuario	Controles para Control de Acceso, Gestión de acceso de usuario, sistema y aplicación y Responsabilidades de Usuario
7	Tecnología Criptográfica	Controles relacionados a cifrado y gestión de llaves
8	Seguridad Física de los Sitios y Equipos de la Organización	Controles que definen áreas seguras, controles de entrada, protección contra amenazas, seguridad de equipo, disposición final segura, escritorio limpio y política de pantalla limpia
9	Seguridad Operacional	Controles relacionados a la gestión de Producción TI, gestión de cambios, gestión de capacidad, malware, respaldos, registros, monitoreo, instalación y vulnerabilidades
10	Comunicaciones y Transferencia de Datos Seguros	Controles relacionados a la seguridad de red, segregación, servicios de red, transferencia de información y mensajería
11	Adquisición, desarrollo y soporte de sistemas de información seguros	Controles que definen requerimiento de seguridad y seguridad en proceso de desarrollo y soporte
12	Seguridad para proveedores y terceros	Controles en que debe incluirse en los acuerdos o contratos y como monitorear a los proveedores y terceros
13	Gestión de incidentes de	Controles para reportar eventos y debilidades, definiendo

No.	Dominio	Descripción
	seguridad de la información	responsabilidades, procedimientos de respuesta y colección de evidencia
14	Gestión de Continuidad del Negocio	Controles para requerimiento de planeación de continuidad de negocio, procedimientos, verificación y revisión y redundancia de TI
15	Cumplimiento	Controles requiriendo la identificación de las leyes y regulaciones aplicables, protección de propiedad intelectual, protección de información personal y revisiones de seguridad de la información

Tabla 29. Descripción de Dominios

Selección de Dominios

El modelo de evaluación permite que el equipo implementador seleccione los dominios que se van a evaluar. Para esto el equipo debe seleccionar y justificar la razón porque selecciona o no selecciona cada dominio.

Dominio	Selección (SI/NO)	Justificación

Tabla 30. Plantilla de Selección de Dominios

Evaluación por Dominio

La segunda parte consiste ofrecer a la organización una vista de la evaluación realizada por dominio, para esto se utilizan la tabla resumen por dominio (Ver Tabla 31).

La tabla resumen por dominio únicamente es una forma de presentación de lo documentado en las tablas de registro por criterio y brindan a la organización una vista general por dominio de la madurez de la seguridad de la información basada en cuatros dimensiones que son los criterios del modelo.

A continuación se detalla la plantilla de la tabla resumen por dominio (Ver tabla 30), debe presentarse una por cada dominio seleccionado.

Dominio

Criterio	Iniciado	Básico	Establecido	Gestionado	Optimizado
Gestión Documental					
Automatización					
Aseguramiento					
Medible					

Tabla 31. Plantilla de Resumen por Dominio

Evaluación Global del Dominio

Para poder evaluar globalmente al dominio, el modelo asigna a cada criterio 25 puntos máximo, definiendo de esta manera que cada criterio tiene la misma ponderación y cada nivel de madurez de cada criterio tendría un valor desde 5 puntos y que al pasar a un nivel superior tendría 5 puntos más hasta alcanzar el máximo nivel del criterio que se ha determinado en 25.

Para calificar de forma global el dominio, se calcula el valor promedio de los cuatro criterios y dependiendo del resultado del valor promedio se califica el dominio globalmente de acuerdo a la siguiente tabla (Ver tabla 32):

Nivel de Madurez Global del Dominio					
Resultado de Valor Promedio	**5**	**10**	**15**	**20**	**25**
Nivel de Madurez	**Iniciado**	**Básico**	**Establecido**	**Gestionado**	**Optimizado**

Tabla 32. Nivel de Madurez Global del Dominio

4.5 Fase V Ejecutar Evaluación de Seguridad

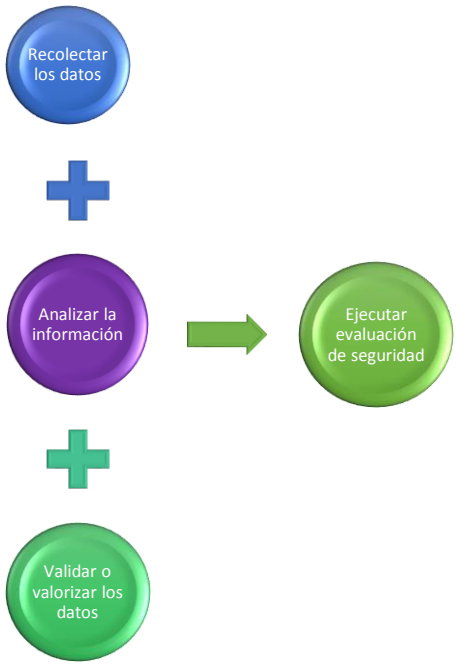


Figura 29. Fase V Ejecutar evaluación de seguridad

Fase de ejecución de la evaluación consiste en llevar a cabo la evaluación a la organización utilizando un instrumento o técnica de recolección de información, metodología de análisis de información y en última instancia valorizar o validar los datos. El equipo lleva a cabo la evaluación de una manera que minimice el impacto de las operaciones de la organización.

4.5.1 Recolectar los datos

La fuente de recolección de datos para la evaluación de la seguridad principalmente son las entrevistas, ya que proporcionan información sobre los dominios de la seguridad de la

información personalizada de la madurez dando adicional conocimiento de la información en la documentación, la observación de las actitudes del entrevistado, su lenguaje corporal o profundizar un tópico como proceso de valoración o validación. Para una mayor precisión en la medición de esta información, se recomienda que todas las entrevistas incluyan dos miembros del equipo para garantizar la documentación completa y la comprensión de todos los comentarios del entrevistado. Un miembro del equipo implementador establece los horarios de las entrevistas necesarias basándose en horarios de los entrevistados y el entrevistador. En los casos en que una entrevista no se puede programar, se debe hacer un intento para programar horarios alternativos según lo permitido e inmediatamente poner la situación en conocimiento de la gestión de su caso para su respectiva resolución.

El equipo debería asegurar un muestreo adecuado de entrevistas debidamente programado de acuerdo a los dominios establecidos a evaluar. Una sesión de la entrevista por lo general requiere de 45 a 60 minutos, dependiendo del nivel de participación del entrevistado y experiencia en la implementación de los dominios de la seguridad de información. Los entrevistadores deben tratar de realizar la entrevista en 45 minutos respetando el tiempo del entrevistado.

Cabe mencionar que el modelo no limita al uso de la entrevista, el equipo implementador puede hacer uso de otro tipo de instrumento que considere conveniente para recolectar la información como por ejemplo cuestionario, observación directa, grupos focales, videos, entre otros.

En esta etapa el equipo implementador debe diseñar el instrumento que se ha decido utilizar en base principalmente a lo que se planifico en la fase anterior, apoyado de la información requerida en las tablas de evidencia de nivel de madurez que el modelo plantea.

4.5.2 Analizar la información

Con base en la información obtenida de las entrevistas, la observación directa, otro instrumento y revisiones de documentos que respaldan cada dominio, los miembros del equipo implementador realizaran el análisis de la información recolectada con el objetivo de determinar que se cuente con toda la información requerida para realizar en la siguiente etapa la valoración de cada dominio en las cuatro dimensiones o criterios planteados. En caso no se cuente con toda la información, el equipo implementador puede realizar algún tipo de ajuste o requerir más información complementaria a la organización de manera que complete toda la información requerida.

4.5.3 Valorizar los datos

Los miembros del equipo implementador determinarán el estado de la madurez de seguridad de información para cada dominio. Además, los miembros del equipo durante las fases de recolección y análisis de la información identificaran los problemas de seguridad de la información, las acciones correctivas lo que les permitirá realizar recomendaciones en un plan de acción correctiva.

Para el modelo de madurez existen cuatro *tablas de evidencia de nivel de madurez,* una por cada criterio de evaluación que plantea el modelo. En cada tabla se encuentra los cinco niveles de madurez que define el modelo por cada criterio y las posibles evidencias por nivel de madurez que se deben encontrar para poder valorar el dominio en el nivel de madurez que le corresponde, según lo descrito anteriormente en la descripción de los criterios.

Para el registro de la evidencia o los hallazgos, el evaluador deberá auxiliarse de las tablas 20 a la 27 descritas anteriormente.

La *tabla de registro* tiene por objetivo registrar o documentar con evidencia el nivel de madurez que cada dominio tiene desde la perspectiva de cada criterio.

Una vez completadas las tablas se deberá ofrecer a la organización una vista de la evaluación realizada por dominio, para esto se utilizan la *tabla resumen por dominio*.

La *tabla resumen por dominio* únicamente es un forma de presentación de lo documentado en las tablas de registro por criterio y brindan a la organización una vista general por dominio de la madurez de la seguridad de la información basada en cuatros dimensiones que son los criterios del modelo.

4.6 Fase VI Verificar los resultados obtenidos

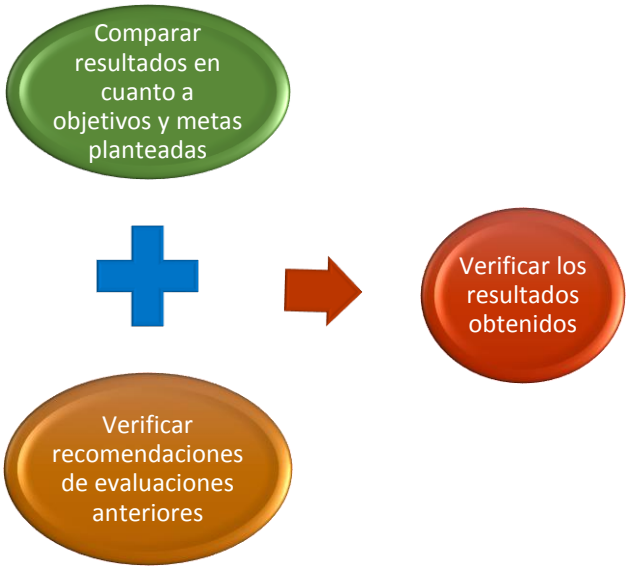


Figura 30. Fase VI Verificar los resultados obtenidos

Cada dominio identificado en el alcance de la evaluación se determina sobre la base de pruebas objetivas:

- La evidencia objetiva recolectada de los diferentes criterios para cada dominio de evaluación debe ser suficiente para cumplir con el propósito de la evaluación y alcance.
- La evidencia objetiva que apoya el juicio de los evaluadores para la calificación de los dominios debe ser registrada. Este registro proporciona pruebas para justificar las calificaciones y para verificar el cumplimiento del procedimiento establecido.
- La obtención de la información de las entrevistas realizadas a las áreas de la organización evaluadas.
- Haciendo uso de los resultados de evaluaciones históricas.

- Desarrollo de sesiones de retroalimentación para validar la información recogida.

4.6.1 Comparar resultados en cuanto a objetivos y metas planteadas

Esto permitirá comparar los objetivos y las metas de madurez planteadas con las encontradas en la realidad, de esta manera se puede determinar la desviación obtenida con la máxima permitida por la organización para establecer sus planes de acción para mejorar la madurez de la seguridad de la información.

4.6.2 Verificar recomendaciones de evaluaciones anteriores

Una parte importante en el proceso de evaluación de la madurez de la seguridad de la información es la mejora continua, para ello debe llevarse un historial de las evaluaciones realizadas que permitan llevar un registro de las recomendaciones sugeridas para así verificar que la Organización ha realizado un avance para mejorar en el dominio recomendado.

4.7 Fase VII Entregar resultados y Presentación de Informes

Figura 31. Fase VII Entregar los resultados y presentación de informes

Durante esta fase, los resultados de la evaluación se analizan y se presentan en un informe. El informe abarca todas las cuestiones principales planteadas durante la evaluación como las zonas observadas fuertes y débiles y las conclusiones de alto riesgo.

En la preparación del informe de evaluación, se debe resumir los resultados de la evaluación, destacando los perfiles de procesos, resultados claves, puntos fuertes y débiles, los factores de riesgo identificados, y acciones de mejora potenciales observados.

Se debe presentar los resultados de la evaluación a los participantes. Además se deben presentar los resultados de la evaluación a la parte interesada. Los resultados de la evaluación también serán compartidos con las partes (por ejemplo, gestión de unidad organizativa) especificadas por la parte interesada.

Finalizar el informe de evaluación y distribuir a las partes pertinentes.

Verificar y documentar que la evaluación se realizó de acuerdo a los requisitos.

Montar el Registro de Evaluación. Proporcionar el Registro de Evaluación para las partes interesadas para su retención y el almacenamiento.

Proporcionar la retroalimentación necesaria de la evaluación como un medio para mejorar el proceso.

4.8 Fase VIII Realizar Ajustes a la Seguridad de la Información

Figura 32. Fase VIII Realizar ajustes a la seguridad de la información

En esta fase se deberá corregir, adaptar o perfeccionar los procesos para su optimización, manteniendo un enfoque proactivo y de mejora continua. La importancia de esta fase radica en ir avanzando hacia el nivel de madurez deseado por la organización.

CAPITULO 5: ANALISIS DE LOS RESULTADOS OBTENIDOS

5.1 Diseño Del Guion De La Entrevista

Para el desarrollo de esta investigación se realizó un guion de entrevista (ver anexo A), el cual se dividió en tres secciones, la primera parte tenía como objetivo, explorar al entrevistado y el área en que se desenvuelve en la organización. Para la segunda parte se pretendía abarcar diferentes objetivos, como: Identificar el grado de importancia de la Seguridad de la Información para la organización, conocer las formas de medir la Seguridad de la Información dentro de la organización y establecer las generalidades de conocimiento sobre Modelos de Madurez de la Seguridad de la Información. Finalmente, en la tercera parte se buscaba identificar el grado de comprensión y el grado de aceptación del modelo propuesto, por los expertos de seguridad de la información, valorizar el modelo de madurez de la seguridad de la información propuesto y establecer propuestas de mejoras al modelo para revalorizarlos.

Para realizar la entrevista se tomó como partida una muestra de 25 empresas de diversos sectores, de las cuales solo 11 empresas nos brindaron colaboración en la realización de la misma.

Para una mejor comprensión el análisis se ha dividido en tres partes, primero se presenta el análisis de los datos generales, posteriormente el análisis del modelo de madurez propuesto y finalmente el análisis de los objetivos planteados.

5.2 Análisis De Datos Generales

La entrevista se realizó a diferentes profesionales dentro del área de Tecnologías de la Información y Seguridad de la Información, como se aprecia en el grafico 1, destacando más a los profesionales de seguridad y consultores. Esto nos permitió dirigirnos a profesionales que tuvieran poco o mucho conocimiento sobre el tema y garantizar que conocieran la problemática de la seguridad de la información que se vive en el país actualmente.

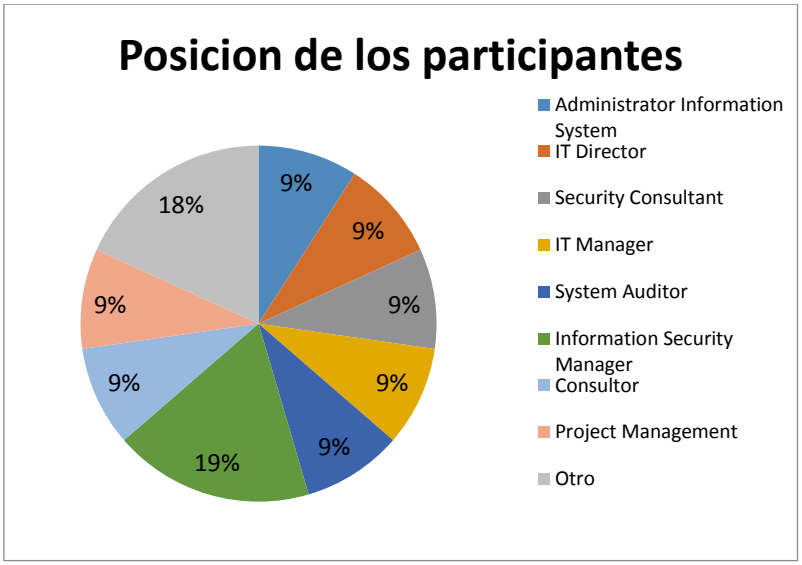


Gráfico 1. Posición de los participantes

Las organizaciones que fueron entrevistadas la mayoría pertenece al sector privado, como se puede apreciar en el gráfico 2, además la mayoría de las personas entrevistadas pertenecían al giro de servicios y área financiera, como se aprecia en el gráfico 3; lo que nos permite conocer la forma en que consideran la seguridad los principales sectores económicos del país.

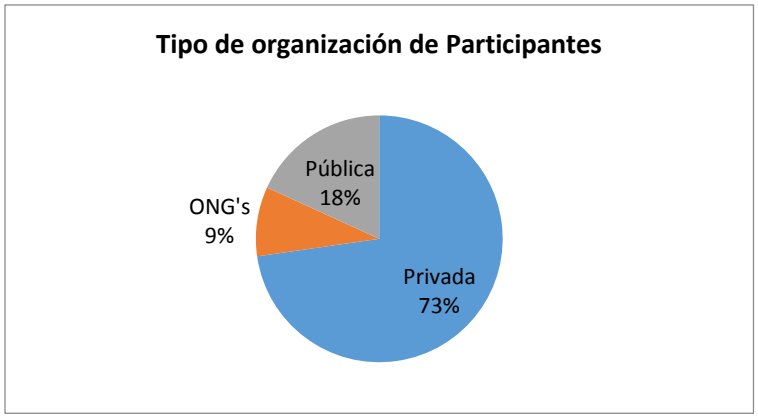


Gráfico 2. Tipo de Organización

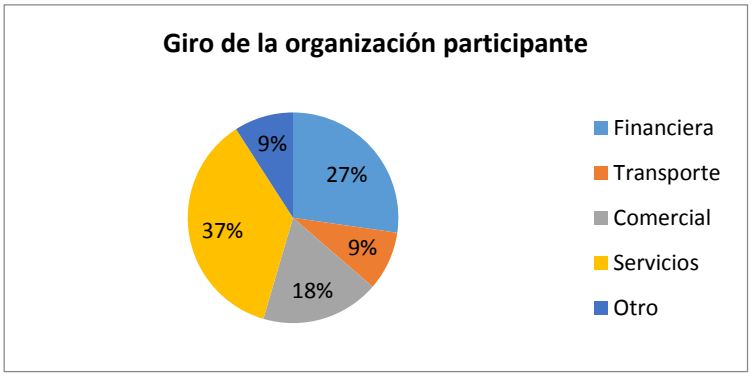


Gráfico 3. Giro de la organización participante.

Una característica importante a destacar en la entrevista es que independientemente del sector al que pertenecían, la mayoría expresaba que para su organización la Seguridad de la información era un punto importante (ver gráfico 4), sin embargo a pesar de ello casi la mitad de ellas poseían alguna herramienta o método para medir la seguridad de la información (ver gráfico 5).

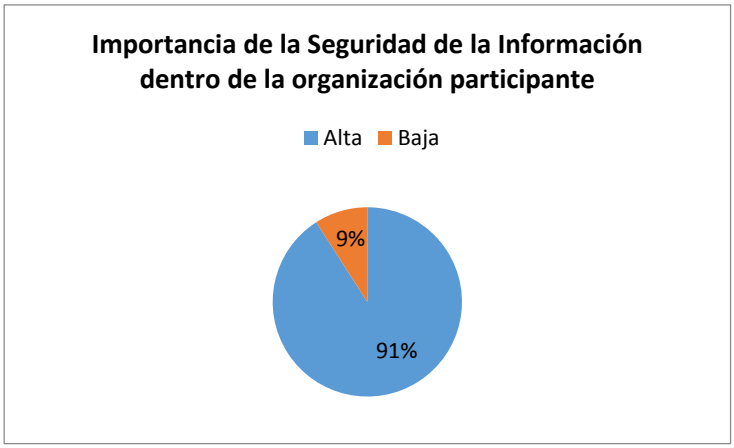


Grafico 4. Importancia de la organización

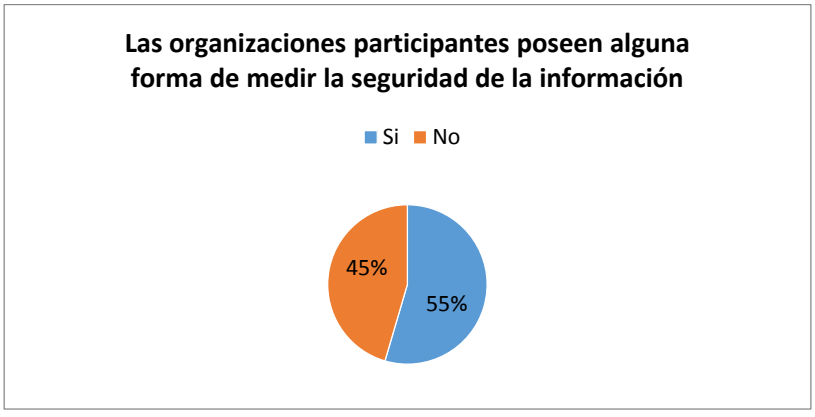


Grafico 5. Las organizaciones poseen alguna forma de medir la seguridad de la información

A pesar que los profesionales de seguridad consideran que la información es importante y conocen sobre la existencia de modelos de madurez actualmente no utilizan ninguno dentro de sus organizaciones, como se aprecia en los gráficos 6 y 7.

Gráfico 6. Conocimiento de la existencia de los modelos de madurez

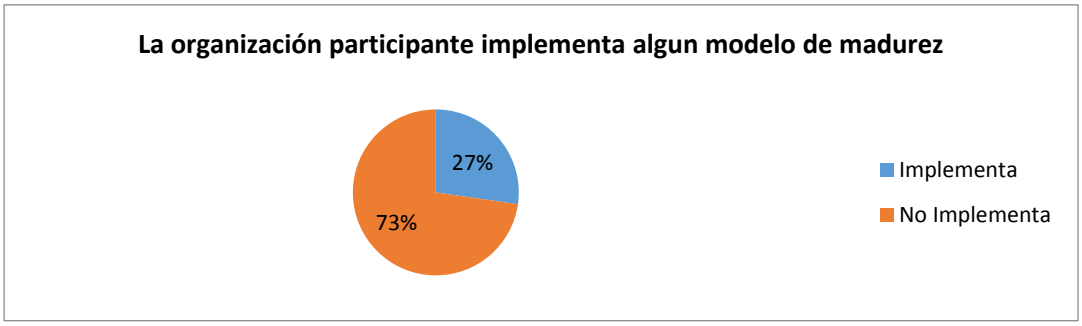


Grafico 7. La organización implementa algún modelo de madurez

5.3 Análisis Del Modelo De Madurez Propuesto

Al presentar la propuesta del modelo de madurez para evaluar la Seguridad de la información a los diversos profesionales se determinó que las fases del modelo propuesto tuvieron una buena aceptación, ya que al presentarle las fases a los expertos de seguridad de la información 73% de ellos consideraron que se encontraban claramente definidas, el gráfico representaba bien al modelo, sin embargo el 27% indico que se deben realizar algunas mejoras con el fin de ayudar a la implementación del mismo. Todos consideraron que era factible su implementación en las diversas organizaciones

Fase I. Contextualizar la seguridad de la información.

Esta fase con sus respectivas sub fases tuvo muy buena aceptación, del 100% de los expertos entrevistados, 73% expresaron que se tenía muy buena comprensión de la fase y sus sub fases, aunque algunos expresaron que aunque este definida claramente debería evaluarse la posibilidad de mejorar la presentación de la misma.

Fase II. Definir el Alcance.

En esta fase consideraron que es de vital importancia para medir la seguridad de la información, porque permite establecer las metas que se van alcanzar, a través de las entrevistas los participantes expresaron que está bien definida y que abarca todos los aspectos necesarios. De los expertos entrevistados, el 73% de ellos consideraron comprensible esta fase, sin embargo hicieron varias sugerencias como replantear sub fases y detallar con mayor precisión los pasos a seguir debido a que si alguien no conoce sobre modelos de madurez podría no ser clara.

Fase III. Establecer roles y responsabilidades.

Esta fase tiene amplia aceptación dentro de los expertos de la seguridad de la información, el 82% de los expertos entrevistados consideraron que se tiene una alta comprensión de la fase y sus sub fases, sin embargo realizaron diversas observaciones para las sub fases, deben ser más descriptivas, tener objetivos claros y definir más sobre cómo se determinaran los equipos.

Fase IV. Planear la evaluación de la seguridad de la información.

Al presentar esta fase, dentro de los expertos hubo muy buena aceptación, el 82% de ellos consideraron altamente comprensible la fase y sub ases, sin embargo realizaron algunas observaciones como ser más descriptivos en las sub fases.

En cuanto a los dominios, los criterios y los niveles de madurez planteados para el modelo de madurez, los expertos consideraron que estaban claros y que es muy bueno que se haya retomado los dominios que plantea la ISO27001.

Fase V. Ejecutar evaluación de la seguridad.

De acuerdo a los expertos, es una fase ampliamente aceptada para la medición de la seguridad de la información, el 91% del 100% de los expertos entrevistados consideraron que la fase y sus sub fases estaban claramente definidas, sin embargo en una de las sub fases se necesita mayor detalle para brindar mayor de claridad y se tuvieron sugerencias para reconsiderar los métodos de recolección de la información.

Fase VI. Verificar los resultados obtenidos.

En general esta fase fue comprendida por los expertos entrevistados, consideraron que se tenía claridad en el objetivo de la fase y sus sub fases, el 73% de los expertos entrevistados expresaron que está claramente definida, sin embargo debe tenerse cuidado de no dejar débil por el tipo de instrumento utilizado para la recolección de los datos.

Fase VII. Entregar resultados y presentación de informes.

Es una de las fases que casi hubo consenso de los expertos entrevistados al expresar que se encuentra claramente definida y es comprensible, el 91% de los entrevistados estuvieron de acuerdo con la definición, solo observaron que debería analizarse la posibilidad de replantear el orden en el que debería ir esta fase.

Fase VIII. Realizar ajustes a la seguridad de la información.

No se tuvo ninguna observación sobre esta fase, todos los entrevistados estuvieron de acuerdo en que la definición es clara y se comprende el propósito de la misma.

5.4 Análisis De Los Objetivos Planteados

Para el desarrollo de este trabajo de investigación se plantearon los siguientes objetivos:

- Proponer un marco de trabajo genérico que permita medir la madurez de la seguridad de la información para la implementación de un modelo facilitando su uso y adaptabilidad al tipo de organización.

  A través de la entrevista a expertos en el área de la seguridad de la información, de diferentes tipos de organización, se determina que el modelo de madurez propuesto puede ser adaptado a cualquier tipo de organización, ya que existe claridad en sus fases y es comprensible lo que facilita su uso.

- Seleccionar la información de fuentes primarias y secundarias de algunos marcos, modelos y/o metodologías de madurez aplicados a la seguridad de la información que sirvan de base para la construcción de un marco de trabajo.

  Se realizó una investigación de diversidad de modelos de madurez existentes, los cuales se plantean en el estado del arte y antecedentes de la investigación, estos nos permitieron contar con una base de conocimientos para poder realizar la propuesta de un modelo de madurez para la seguridad de la información.

- Identificar de qué manera los modelos de seguridad de la información existentes son adaptables, comprensibles y factibles de implementar en organizaciones sin importar su rubro y tamaño.

  A lo largo de toda la investigación se estudiaron diversos modelos de madurez destacando principalmente cinco modelos, los cuales se detallan con profundidad en las Bases Teóricas de la investigación.

- Diseñar un marco de trabajo genérico que permita la implementación de un modelo de madurez que mida la seguridad de la información en una organización.

  De acuerdo a los expertos entrevistados la propuesta del modelo de madurez tiene una gran aceptación, es comprensible y está claramente definido, esto vendría a proporcionar

una gran ayuda a las organizaciones que actualmente no cuentan con una herramienta para medir como se encuentra el estado de la seguridad de la información dentro de sus organizaciones.

CAPITULO 6: CONCLUSIONES DE LOS RESULTADOS Y RECOMENDACIONES

El marco de trabajo genérico propuesto para implementar un modelo de madurez de la seguridad de la información, tiene varias ventajas:

- Fácil comprensión para el equipo implementador, por su sencillez en la descripción de las fases y las actividades que se deben realizar en cada una de ellas.
- Adicionalmente facilita su aplicabilidad, debido a que las fases del marco de trabajo genérico poseen pasos lógicos y secuenciales; esta propuesta no posee flujos que hagan bifurcaciones o ciclos repetitivos en sus procesos de trabajo.

En el estudio de un modelo de madurez de seguridad de la información se han identificado algunos factores importantes de éxito, entre ellos:

- Tener claridad en la definición del alcance, al establecer hasta donde se debe llegar y lo que en realidad no se incluye en el dominio evaluado.
- El apoyo y compromiso de la alta dirección es de suma importancia para el éxito de la implementación del modelo.
- Interés real de la organización por medir la madurez de la seguridad de la información y mejorarla.

En una escala de madurez los nombres de los niveles deben ser descriptivos, para facilidad de comprensión.

Existe una gran necesidad en el ámbito de la Seguridad de la Información, de acuerdo a la investigación bibliográfica realizada y a las entrevistas a expertos de seguridad de la información en el país, sin embargo algunos de los expertos entrevistados su contexto de trabajo es a nivel regional. A pesar de esta realidad las organizaciones no cuentan con herramientas que permitan medir el estado en el que se encuentra la seguridad de la información. Con la propuesta de este modelo de madurez se pretende facilitar a las diferentes organizaciones con una herramienta que les permita implementar una evaluación del estado en que se encuentra la seguridad de la información a través de un modelo de madurez.

Este modelo de madurez como trabajo futuro deberá evaluarse y someterse a las diferentes recomendaciones y sugerencias hechas por los expertos para poder mejorar continuamente dicho modelo y adicionalmente se recomienda hacer una prueba piloto.

BIBLIOGRAFIA

(DOE), U. D. (2014, Febrero). *Energy.gov.* Retrieved Julio 2014, from cybersecurity capability maturity model (c2m2): http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program/cybersecurity

Aceituno, V. (2011, Febrero). Open Information Security Management Maturity Model (O-ISM3). The Open Group.

Arbeláez, R. (2008, Junio). Modelo de Madurez de Seguridad de la Información: cómo debe evolucionar la seguridad en las organizaciones. Colombia: VIII Jornada Nacional de Seguridad Informática ACIS.

Becker, P. D. (2009). Developing Maturity Models for IT Management – A Procedure Model and its Application. *Developing Maturity Models for IT Management – A Procedure Model and its Application*. Germany: European Research Center for Information Systems, University of Münster.

Bobbert, Y. (2010). Maturing Business Information Security. Holanda.

Bowen, P., & Kissel, R. (2007, Enero). Program Review for Information Security Management Assistance (PRISMA). United States of America: National Institute of Standards and Technology (NIST).

Carnegie Mellon University . (2010, Noviembre). CMMI® for Development. *CMMI® for Development*. USA: Carnegie Mellon University .

Carnegie Mellon University. (1999, Abril 1). Systems Security Engineering Capability Maturity Model (SSE-CMM) Model Description Document Versión 2.0. Pittsburgh, Pensilvania, Estados Unidos: Universidad Carnegie Mellon.

Carnegie Mellon University and Software Engineering Institute. (2002). *Capability Maturity Model Integration.* Pittsburgh: Carnegie Mellon University.

Creswell, J. W. (1998). Qualitative inquiry and research design. *Qualitative inquiry and research design*. Sage Publications.

Cuevas. (2009).

David A. Chapin, S. A. (2005). *¿Cómo puede medirse la seguridad?* Retrieved from ISACA Trust in, and value from, information systems: http://www.isaca.org/Journal/Past-Issues/2005/Volume-2/Pages/Como-Puede-Medirse-la-Seguridad.aspx

Daymon. (2010).

Ebrahim Hamad Al-Hanaei, A. R. (2014). DF-C2M2: A Capability Maturity Model for Digital Forensics Organisations. Lancaster, Reino Unido.

Elizabeth Pérez Mergarejo, Y. R. (2013). Procedimiento para la aplicación de un modelo de madurez para la mejora de los procesos. *Revista Cubana de Ingenieria RCI Vol. V No. 2*, 29-39.

Humphrey, W. S. (1987). *Characterizing the Software Process-A Maturity Framework.* Pittsburgh, Pennsylvania: Software Engineering Institute - Carnegie Mellon University.

Humphrey, W. S. (1989). *Managing the Software Process.* Addison-Wesley Professional.

inforc Ecuador. (2011, Octubre 13). *ISACA Presenta el Modelo de Evaluación de Procesos de COBIT*. Retrieved from inforc Ecuador: http://www.inforc.ec/isaca-presenta-el-modelo-de-evaluacion-de-procesos-de-cobit/

ISACA. (2011). COBIT Process Assessment Model (PAM) using COBIT 4.1. *COBIT Process Assessment Model (PAM) using COBIT 4.1*. Rolling Meadows, Illinois, USA: ISACA.

ISO/IEC. (2002, 10 01). Information technology — Systems Security Engineering — Capability Maturity Model (SSE-CMM). *Information technology — Systems Security Engineering — Capability Maturity Model (SSE-CMM)*. Suiza: ISO/IEC 2002.

ISO/IEC. (2013, 10 01). Information technology -- Security techniques -- Information security management systems -- Requirements. *Information technology -- Security techniques -- Information security management systems -- Requirements*. ISO.

Jan Eloff, M. E. (2003). Information Security Management – A New Paradigm. *South African Institute of Computer Scientist and Information Technologists SAICSIT 2003*.

José Antonio Calvo-Manzano, T. S. (2003). Estudio Aplicación del Modelo de Madurez Capacidad de Ingeniería en Seguridad de los Sistemas (SSE-CMM) por áreas de Proyecto y Organización. Madrid, España: Facultad Informática, Universidad Politécnica de Madrid .

Juan Manuel Gers, P., & José Enar Muñoz Narváez, I. (2014). DESARROLLO DE UN MODELO DE MADUREZ EN REDES INTELIGENTES. Weston, Florida, USA. Retrieved from http://gers.com.co/wp-content/uploads/2014/10/Modelos-de-Madurez_rev1.pdf

Linares, S., & Paredes, I. (2007, Mayo 28). Seguridad de la Información a la Mediana Empresa IS2ME. España.

Luís Enrique Sánchez, D. V.-M. (n.d.). Developing a model and a tool to manage the information security in Small and Medium Enterprises. Ciudad Real, España.

Marco Spruit, M. R. (2014). ISFAM: THE INFORMATION SECURITY FOCUS AREA MATURITY MODEL. Telaviv: Twenty Second European Conference on Information Systems.

Marianella Villegas, O. V. (2009, Junio 5). Modelo de Madurez de la Gestión de la Seguridad Informática en el contexto de las Organizaciones Inteligentes. Caracas , Venezuela.

Marten Simonsson, P. J. (2007). Model-Based IT Governance Maturity Assessments with Cobit. Estocolmo, Suecia: European Conference on Information Systems ECIS.

MATRANE, O., TALEA, M., & OKAR, C. (2014). Towards A New Maturity Model for Information Security. *International Journal of Advanced Research in Computer Science and Software Engineering*, 71-78.

Michael E. Whitman, H. J. (2012). *Principles of Information Security.* Boston, MA: Course Technology.

Nobari, B. Z. (2011). Information Security Maturity Model. *La presentación de un modelo para Clasificación de las Organizaciones basada en el Nivel de Madurez de Seguridad de la Información.* Tehran, Iran: I.A.U., Science & Research Branch.

Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993). *Capability Maturity Model, Version 1.1.* Pittsburg Penssylvania: Institute for Software Research Carnegie Mellon University.

Rao, V. (2003, Noviembre 26). An Approach to Implementing Maturity Models in IT Security. Perth, Australia : University of New South Wales.

Roberto Hernandez Sampieri, C. F. (2010). *Metodología de la Investigación.* D.F. México: McGrawHill.

Roberto Hernández Sampieri, C. F. (2010). Metodología de la Investigación. In R. H. Sampieri, *Metodología de la Investigación.* México: McGraw-Hill.

Saavedra, A. –B.–G. (2006). *CMM – Capability Maturity Model.* Ingenieria de Software – U.N.C.P.B.A.

Saleh, M. F. (2011). Information Security Maturity Model. *International Journal of Computer Science and Security (IJCSS), 5*(3), 316-337.

Sánchez, L. E., Villafranca, D., Fernández-Medina, E., & Piattini, M. (2009, Marzo). Developing a model and a tool to manage the information security in Small and Medium Enterprises. Ciudad Real, España.

Sanchez, L. E., Villafranca, D., Fernandez-Medina, E., & Piattini, M. (2009). MGSM-PYME: Metodología para la gestión de la seguridad y su madurez en las PYMES. Ciudad Real, España: Universidad Castilla-La Mancha.

Schulz, W. H. (1987). *A Method for Assessing the Software Engineering Capability of Contractors .* Pittstburg Penssylvani: Software Engineering Institute Carnegie Mellon Institute.

Symantec. (n.d.). Symantec Security Program Assesment. *2008*. California, USA: Symantec.

van Steenbergen, M., Bos, R., Brinkkemper, S., van de Weerd, I., & Bekkers, W. (2010). The Design of Focus Area Maturity Models. *6105*, 317-332. Lecture Notes in Computer Science, Springer.