Unidad 2 / Escenario 4

Lectura fundamental

Modelos modernos de seguridad de la información

Contenido

Palabras clave: BMIS, O-ISM3, negocio, procesos, niveles de capacidad, niveles de madurez.

Hemos visto la evolución en temas de seguridad de la información con la revisión de los modelos tradicionales que surgieron por las necesidades militares y comerciales de la época. Sin embargo, este enfoque de seguridad de la información ha cambiado. Las empresas se encuentran en constante riesgo debido al uso masivo de internet y de dispositivos móviles para acceder en cualquier momento y lugar a la información, a la colaboración empresarial y el comercio electrónico, entre otros factores.

En este sentido, las empresas deben prepararse no solo para proteger la integridad y confidencialidad de la información, sino para ampliar el alcance de la seguridad en lo referente a la disponibilidad; esto con el fin de cumplir requisitos normativos, hacer frente a las exigencias del mercado y realizar una eficiente gestión de riesgos que les permita cumplir sus objetivos empresariales.

Así, han surgido nuevos modelos en seguridad de la información, en los cuales la seguridad no es pensada solo en términos de acceso, sino que involucra temas de estrategia empresarial y responsabilidad compartida; además, consideran que la seguridad no debe ser una responsabilidad del área de TI únicamente, la cual es solo un facilitador y una parte del proceso. Así, el enfoque moderno de la seguridad de la información es que esta no es un gasto más, sino una herramienta que al gestionarse eficientemente permite el cumplimiento de los objetivos empresariales, mejora la eficiencia en la prestación de los servicios y se alinea completamente con los objetivos comerciales.

A continuación, veremos dos modelos que tienen dicho enfoque y que están pensados desde lo estratégico para la protección de los activos de información.

1. Modelos ISM3

The Open Group desarrolló el modelo *Information Security Management Maturity Model* (ISM3) o O-ISM3, el cual ya se encuentra en su segunda versión. Este se caracteriza por ser un modelo de capacidades. Con O-ISM3, la empresa intenta alcanzar un nivel de seguridad definido o riesgo aceptable en lugar de buscar la eliminación de vulnerabilidades, puesto que hace de la seguridad un proceso medible mediante el uso de indicadores de gestión. O-ISM3 define que el propósito de la seguridad de la información es garantizar el cumplimiento de los objetivos de negocio. Por ello, los relaciona directamente (por ejemplo, presencia Web) con el programa de seguridad de la organización.

1.1. Historia

Un modelo de madurez es un conjunto estructurado de elementos que permite identificar en qué grado el ente de evaluación ha alcanzado un objetivo o ha logrado un grado de madurez frente a un tópico determinado.

Los modelos de madurez posibilitan establecer en dónde estamos hoy a través del autoanálisis y la comparación con la competencia o *benchmarketing* y, de acuerdo con los objetivos planteados, definir dónde debo estar por medio de alineación de objetivos estratégicos con requerimientos presentes y futuros.

Bajo esta consideración, The Open Group ha desarrollado el estándar abierto para la gestión de seguridad de la información o modelo de madurez de seguridad de la información ISM3. The Open Group es un consorcio global que faculta el logro de los objetivos comerciales a través de los estándares de TI. Con más de 500 organizaciones miembros, tiene una diversidad de membresías que abarca todos los sectores de la comunidad de TI: clientes, proveedores de sistemas y soluciones, proveedores de herramientas, integradores y consultores, así como académicos e investigadores.

Desde el año 2003, The Open Group ha trabajado en el modelo por medio de un grupo de investigadores, consultores y miembros de la comunidad, siendo su versión tres la más reciente, liberada en 2017 (Canal, 2017).

1.2. Elementos

1.2.1. Metas

En la figura 1 se presentan los 3 tipos de metas que el modelo identifica como importantes para gestión de seguridad con un enfoque gerencial:

- **Metas de negocio:** objetivos estratégicos que la empresa define como su razón de ser y por los cuales nacen las demás actividades, procesos y procedimientos de la empresa.
- **Metas de seguridad:** son derivadas del negocio y se encuentran influenciadas por las necesidades y limitaciones a nivel regulatorio o técnico. Estos son los objetivos del sistema de gestión de seguridad de la información.
- **Metas de calidad:** son derivadas del negocio y representan los objetivos del sistema de gestión de calidad de la empresa, si existe. Es importante considerar estas metas para alinearlas con las metas de seguridad (ACIS, 2017).

Figura 1. Metas del modelo O-ISM3

Fuente: elaboración propia

1.2.2. Orientación por procesos

O-ISM3 está orientado a procesos, por lo cual es compatible con otras buenas prácticas y estándares como ISO27001, Cobit, Itil e ISO9001.

Todo lo que O-ISM3 hace se centra en el concepto del proceso. Los procesos tienen capacidades y se administran utilizando prácticas de gestión.

O-ISM3 identifica cuatro niveles de procesos o gestión de seguridad. El nivel inferior reporta al nivel superior. Los niveles de gestión son:

- Genérico: para gestión general.
- Estratégico (dirigir y proporcionar): se ocupa de objetivos amplios, coordinación y provisión de recursos.
- Táctica (implementar y optimizar): se ocupa del diseño e implementación del SGSI, objetivos específicos y gestión de recursos.
- Operacional (ejecutar e informar): se ocupa de alcanzar metas definidas por medio de procesos técnicos.

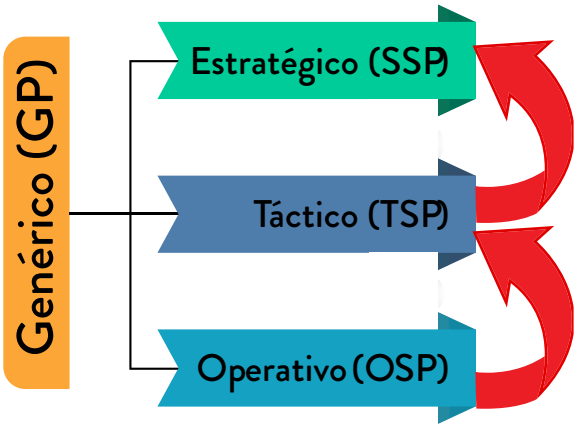

Figura 2. Procesos O-ISM3

Fuente: elaboración propia

Para que una responsabilidad se lleve a cabo correctamente dentro de un proceso y según el modelo, la persona o el equipo deben ser:

- Responsable (tener un interés personal en el resultado).
- Competente (tener el conocimiento y la experiencia).
- Motivado (influenciado por la voluntad de tener éxito).
- Empoderados (tener recursos y la libertad de tomar decisiones y dar retroalimentación).

Las métricas de los procesos deben estar orientadas a confirmar la efectividad del proceso desde sus actividades, alcance, calidad, eficiencia y efectividad (The Open Group, 2017).

1.2.3. Niveles de capacidad

Capacidad, para el modelo, hace referencia a los atributos que tiene la empresa para ejecutar un proceso. Desde una perspectiva gerencial, entre más alta la capacidad, mejor es la adopción del modelo en cuanto a la aplicación de los procesos definidos. Desde la perspectiva de un auditor, el nivel de capacidad de la empresa se mide por la documentación del proceso y las métricas utilizadas para su gestión.

1.2.4. Niveles de madurez

Son combinaciones específicas de niveles de capacidad y procesos. Los procesos se asignan a niveles de madurez certificables de acuerdo con un espectro, desde un ISM3 básico hasta uno avanzado. Existe una relación entre la cantidad de procesos, su capacidad y la madurez del SGSI. Cuantos más procesos y mayor sea la capacidad, mayor será la madurez. Las relaciones clave detrás de los niveles de madurez O-ISM3 son:

- Mapeo (o agrupamiento) de procesos en cada O-ISM3 nivel de madurez.
- Definir la capacidad por cada proceso de mapeo en cada O-ISM3 nivel de madurez.

Los niveles de madurez están diseñados para adaptarse a las necesidades de las organizaciones con diferentes tamaños, recursos, amenazas, impactos, apetitos de riesgo o sector económico.

1.3. Estructura

O-ISM3 proporciona un marco para construir, adaptar y operar un sistema de gestión de seguridad de la información (ISMS). El uso de las métricas garantiza que este utilice de manera eficiente criterios cuantitativos objetivos para informar las decisiones empresariales sobre la asignación de recursos de seguridad de TI y la respuesta a los cambios. Los beneficios para la seguridad de la información son un menor riesgo y un mejor retorno de la inversión (ROI).

En este sentido, su estructura se encuentra alineada con los procesos que propone el modelo, teniendo en cuenta las capacidades de la empresa (desde el punto de vista de los procesos) y el nivel ISM3 que se espera alcanzar conforme a sus necesidades y capacidades.

En la tabla 1 se evidencia un resumen de la estructura general del modelo según *The Open Group (2017)*, considerando los niveles de capacidad, las métricas a cumplir por cada nivel de capacidad y las actividades de gestión que deben realizarse por cada uno de los niveles de capacidad.

Tabla 1. Estructura del Modelo O-ISM3

Nivel de capacidad		Inicial	Gestionado	Definido		Controlado		Optimizado
Actividades de Gestión		Auditar, certificar	Probar (Evaluar)	Planear	Monitorear	Analizar beneficios	Mejorar la calidad	Mejorar el desempeño
Documentación		*	*	*	*	*	*	*
Tipo de Métrica	Actividad			*	*	*	*	*
	Alcance			*	*	*	*	*
	Efectividad			*	*	*	*	*
	Calidad					*	*	*
	Carga (peso)							*
	Eficiencia							*

Fuente: elaboración propia

1.3.1. Niveles de capacidad

- **Inicial:** el proceso o la labor que puede usarse no se ha establecido y apenas se va a concretar.
- **Gestionado:** el proceso se encuentra establecido, es posible gestionarlo, pero falta su definición o documentación.
- **Definido:** el proceso es usado y se encuentra documentado.
- **Controlado:** el proceso se encuentra definido, es gestionado y arroja métricas para su mejoramiento.
- **Optimizado:** el proceso se encuentra controlado y el mejoramiento ha sido aplicado para optimizar el uso de los recursos (Canal, 2010).

1.3.2. Niveles de madurez

- **ISM3 Nivel 1:** inversión mínima en los procesos esenciales del ISMS. Diseñado para organizaciones con bajos objetivos de seguridad en ambientes de bajo riesgo. Se reduce el riesgo proveniente de amenazas técnicas.
- **ISM3 Nivel 3:** inversión importante en los procesos esenciales del ISMS. Diseñado para empresas con altos objetivos de seguridad en ambientes de riesgos normales o altos. Se reduce el riesgo a niveles más bajos que el nivel 1, proveniente de amenazas técnicas.
- **ISM3 Nivel 5:** inversión alta y optimizada en los procesos esenciales del ISMS. Diseñado para empresas con altos objetivos de seguridad y requerimientos específicos en ambiente de riesgos.

1.3.3. Métricas

La métrica es una medida que puede ser interpretada de acuerdo con una línea base o mediciones previas. En términos de procesos, ayuda a la toma de decisiones y mejoramiento de ellos.

O-ISM3 define los siguientes tipos de métricas:

- **Métricas de actividad:** estas cuentan la cantidad de entregas que son entradas y salidas de un proceso en un período de tiempo. Para algunos casos, entre más alto sea su valor es mejor; por ejemplo, cantidad de capacitaciones, donde el volumen de esta actividad puede ser una métrica de calidad. Para otros casos, una actividad rápida conducirá a mejores resultados que su cantidad; por ejemplo, cuenta de usuario creada, en donde la métrica de calidad es la satisfacción del usuario por la respuesta dada.
- **Métricas de alcance:** estas comparan la cantidad de entregables, que son entradas, con el total de entradas posibles. Para ciertos procesos, en cuanto mayor sea el alcance (cantidad de entregables), mayor es el valor. Por ejemplo, si se quiere probar un *malware*, entre más dispositivos se utilicen para la prueba, mayor sensación de seguridad.
- **Métricas de efectividad:** estas comparan la cantidad de entregables, que son entradas, con el número de salidas. Para ciertos procesos, entre menos entradas mejor. Por ejemplo, una menor cantidad de solicitudes de eliminación de virus cumplidas identifica mayor seguridad de la herramienta. Si aumenta la salida, algo sucede en la red.
- **Métricas de calidad:** estas comparan el resultado final del proceso con el objetivo inicial. La actividad, el alcance y la efectividad pueden ser métricas de calidad, según el proceso, en un período de tiempo.
- **Métricas de carga:** estas comparan los recursos utilizados realmente en el proceso vs. los recursos presupuestados. Adicionalmente, contrasta el número de entradas efectivas con la cantidad de entradas definidas previamente en un tiempo determinado. Por ejemplo, una carga baja en un proceso puede indicar que los recursos deben reasignarse para optimizar su uso.
- **Métricas de eficiencia:** estas comparan el resultado del proceso con los recursos estimados para ejecutarlo. Es decir, la relación entre los entregables, los recursos utilizados y la cobertura que el resultado proporciona. Por ejemplo, la cantidad de *backup* que se realiza con un mínimo de recursos y contemplando toda la organización; entre mayor sea el número, mayor eficiencia. La eficiencia debe evaluarse también bajo los parámetros de calidad (el *backup* debe incluir unos mínimos para que sea aceptable). Un proceso puede ser efectivo (cumple con su objetivo) pero no eficiente (utiliza más recursos de los esperados para alcanzar el objetivo) (The Open Group, 2017).

1.3.4. Actividades de gestión

- **Gestión del conocimiento:** llevar registros, promover acuerdos y compartir conocimientos, generalmente basados en documentación.
- **Auditoría:** los controles se realizan con base en la evidencia de si las entradas del proceso, las actividades y los resultados coinciden con su documentación.
- **Certificar:** la certificación evalúa (usando evidencia) si la documentación del proceso, los insumos, los productos y las actividades cumplen con un estándar, ley o regulación predefinida.
- **Pruebas:** evalúan si las salidas del proceso son el resultado esperado cuando se ingresan datos de prueba.
- **Planificación:** organización de las actividades a realizar, asignación de hitos, recursos, presupuesto y métricas de los procesos.
- **Monitoreo:** verificar si las entradas a un proceso, las salidas del proceso y los recursos utilizados por el proceso se encuentran dentro del rango normal o de acuerdo con los planes de trabajo, usando métricas para detectar anomalías significativas y tomando decisiones para corregirlos.
- **Análisis de beneficios:** muestra cómo el logro de los objetivos de seguridad contribuye al alcance de los objetivos comerciales; mide el valor del proceso para la organización o justifica el uso de los recursos.
- **Mejora de la calidad:** realizar cambios en el proceso para hacerlo más adecuado para el propósito, eliminando fallas antes de que produzcan incidentes.
- **Mejora del rendimiento:** hacer cambios en el proceso para reducir el uso de recursos (The Open Group, 2017).

1.4. Aplicaciones

El modelo se puede aplicar en cualquier industria y tipo de organización. Por ser un modelo de madurez, las organizaciones definen el nivel de cumplimiento que quieren alcanzar y su avance, si sus necesidades lo requieren.

Para la aplicación del modelo en el contexto de seguridad, se sugiere seguir lo indicado en la figura 3, lo cual propone The Open Group (2017):

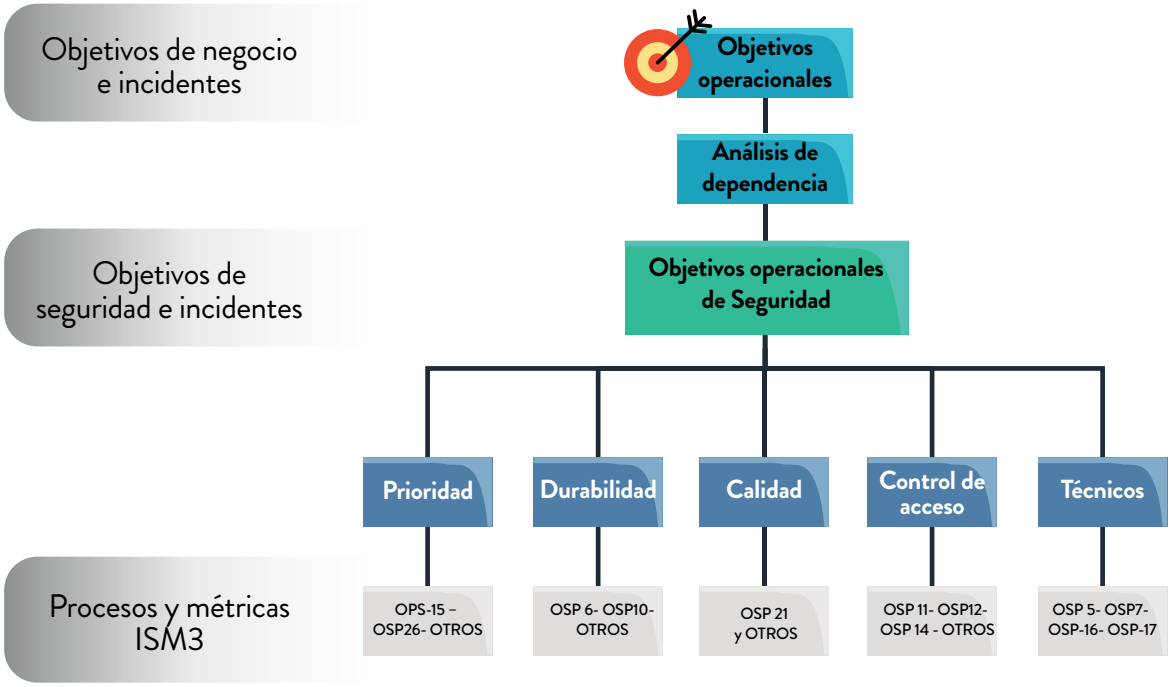

Figura 3. Modelo de seguridad O-ISM3

Fuente: elaboración propia. Modificado de The Open Group, 2017

En términos generales, acorde con The Open Group (2017), el modelo propone los siguientes procesos como fundamentales para alcanzar el primer nivel de madurez:

- GP-1: *Knowledge Management*
- GP-3: *ISM Design and Evolution*
- SSP-1: *Report to Stakeholders*
- SSP-2: *Coordination*
- SSP-6: *Allocate Resources for Information Security*
- TSP-1: *Report to Strategic Management*
- TSP-2: *Manage Allocated Resources*
- TSP-3: *Define Security Targets*
- TSP-4: *Service-Level Management*
- OSP-1: *Report to Tactical Management*
- OSP-5: *IT Managed Domain Patching*

- OSP-11: *Access Control*
- OSP-16: *Segmentation and Filtering Management*
- OSP-17: *Malware Protection Management*
- OSP-10: *Backup Management*
- OSP-21: *Information Quality and Compliance Probing*

2. Modelo de negocio de seguridad de la información

El modelo de negocio de seguridad de la información (BMIS por sus siglas en inglés *Business Model for information Security)* apoya a las empresas, específicamente el *core* de su negocio, en lo referente a seguridad de la información. Su enfoque, desde lo estratégico, utiliza el pensamiento sistémico para explicar el funcionamiento de la empresa y la construcción de sus relaciones con el fin de gestionar la seguridad de manera eficiente. Los elementos y las interconexiones dinámicas que conforman la base del modelo establecen los límites de un programa de seguridad de la información, presentando una visión holística y dinámica para el diseño, implementación y gestión de un sistema de seguridad de la información (ISACA, 2009).

2.1. Historia

ISACA, *Information Systems Audit and Control Association*, es una asociación global sin ánimo de lucro de 140.000 profesionales en 180 países, que fue fundada en 1969 con el fin de ofrecer conocimiento, estándares, relaciones, acreditación y desarrollo en temas de gobierno de TI, ciberseguridad y gestión de seguridad de la información, entre otros.

En el año 2008, ISACA celebró un acuerdo formal con la Universidad del Sur de California (EE. UU.) y el Marshall School of Business Institute para la protección de infraestructura crítica, con el fin de continuar su investigación sobre el desarrollo de un modelo de gestión sistémica de seguridad.

La investigación duró alrededor de 2 años; el 06 de octubre de 2010 fue lanzado oficialmente el modelo de negocio para seguridad de la información. El objetivo de ISACA ha sido transformar un modelo teórico a una herramienta práctica con el propósito de unir los proyectos de seguridad de la información de las empresas con la estrategia organizacional, debido a que se invierte demasiado tiempo intentando brindar soluciones de tipo reactivo que se convierten en alivios de corto plazo, centradas principalmente en la tecnología, desconociendo los cambios del entorno. Este tipo de soluciones no son pensadas para ser sostenibles en el tiempo, lo que genera debilidad en la seguridad, mal gobierno, personal sin competencias o cultura disfuncional, temas que son abordados en el modelo de seguridad (Kessinger, 2010).

2.2. Elementos

Los elementos del modelo se resumen en una figura tridimensional en forma de pirámide (ver figura 4), en la cual estos deben ser considerados en todo momento para no perder el equilibrio. Las interconexiones o lados de la pirámide brindan soporte a los elementos para que el modelo se adapte según sus necesidades. Adicionalmente, estas conexiones son el resultado del enfoque global sistémico, lo que indica que pueden verse afectadas no solo por los elementos de los extremos, sino por cualquier cambio de los componentes.

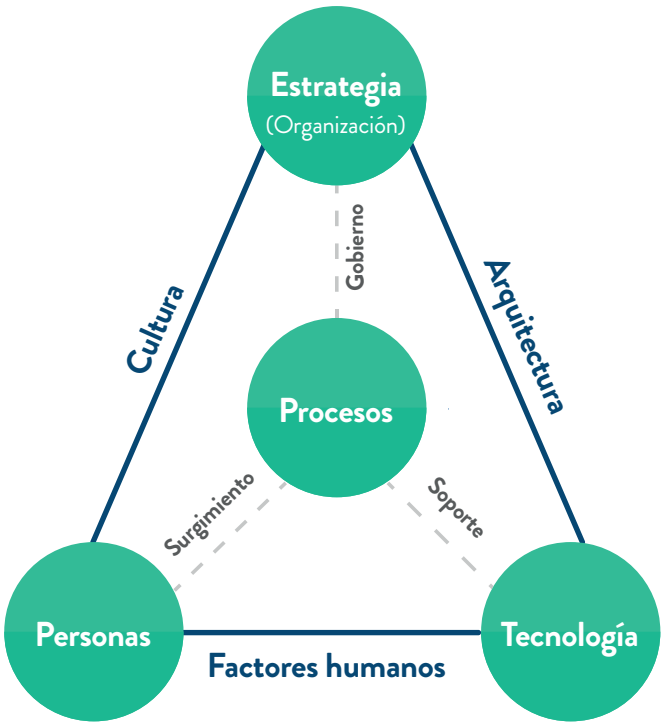

Figura 4. Modelo de negocio seguridad de la información

Fuente: elaboración propia

2.2.1. Diseño y estrategia de la organización

Es la cabeza del modelo, lo cual expresa la importancia de los objetivos de la organización. La estrategia es la ruta de navegación de una empresa, que señala a dónde se quiere ir, cómo se espera navegar y qué se quiere alcanzar con ese viaje. Es la brújula para lograr el éxito de la empresa. El diseño de la estrategia está determinado por la cultura (personas), su forma de gobierno (procesos) y su arquitectura empresarial (uso de la tecnología), y el material principal para elaborarla son sus recursos humanos, técnicos, operativos, *know how*, entre otros (ISACA, 2009).

En este sentido, esta parte del modelo indica la relación que existe entre las personas, los procesos y la tecnología y cómo la estrategia afecta estos elementos. Dicha relación puede generar riesgos, oportunidades o áreas de mejora que influyen los principios de seguridad. Esta perspectiva es importante pues la empresa se considera como un todo y no como un conjunto de elementos aislados.

2.2.2. Recursos humanos y aspectos de seguridad que lo rodean

Define el o los encargados de implementar la estrategia, lo cual no puede ser realizado solamente por el responsable de seguridad o de tecnología. Es importante alinearse con otras áreas de la organización, como lo son:

1. El área de recursos humanos, para definir políticas de ingreso y retiro.
2. El área jurídica, para establecer roles, responsabilidades, permisos por su función y responsabilidad, motivos de despido, protocolos de salida.
3. El área operativa, para determinar el acceso a herramientas, datos, capacitación y movimientos dentro de la empresa.

Dentro de este elemento también deben ser considerados los proveedores, clientes y/o partes interesadas que pueden influenciar la empresa y, por tanto, deben hacer parte del modelo de seguridad.

2.2.3. Procesos

Son aquellas actividades que realiza la empresa para cumplir con sus objetivos organizacionales; deben incluir los mecanismos formales e informales utilizados para alcanzarlos. Los procesos tienen la gran ventaja de visibilizar la operación, puesto que, si se definen indicadores de gestión para medir su efectividad, son una herramienta potente para controlar riesgos, hacer seguimiento de responsabilidades y operar la organización (ISACA, 2009).

Para que los indicadores sean eficaces deben expresar objetivos medibles, estar documentados, ser comunicados y revisados periódicamente para poder medir su eficiencia y eficacia.

Dentro del modelo, la importancia de los procesos radica en la realimentación que estos pueden brindar al compartir observaciones, preocupaciones y sugerencias entre las personas.

2.2.4. Tecnología

Está conformada por todas las herramientas, elementos, dispositivos, *software* y aplicaciones que se utilizan para desarrollar los procesos o mejorar su eficiencia. Es decir, son el soporte de las actividades que la empresa debe desarrollar para cumplir con sus objetivos estratégicos.

Para muchas organizaciones, la tecnología hace parte de un gasto, el cual se asume por la dependencia que tanto personas como procesos han generado, y que las empresas definen como ganar ventaja competitiva. Sin embargo, por ser solo un "gasto", la elección suele ser deficiente, no satisface las necesidades de la empresa y se ignora si esta, en su conjunto, está preparada y cuenta con la capacidad para asumirlo. Por dicha razón, el modelo propone que, desde la gerencia, la tecnología sea vista como un instrumento para controlar los riesgos en seguridad, sin desconocer que no es la única solución y analizando eficazmente la capacidad de la empresa (personas, procesos) para gestionar los controles definidos.

2.2.5. Conexiones dinámicas

Las interconexiones dinámicas enlazan los elementos mencionados anteriormente y son parte fundamental del modelo.

Cualquier conexión entre dos elementos es flexible y muestra el dinamismo y el patrón sistémico del modelo, que puede generar bucles de realimentación en ciertos puntos; esta realimentación va cambiando de estado a lo largo del modelo. Por todo esto, las interconexiones requieren especial atención y determinan, como tal, la estructura del modelo.

2.3. Estructura

La estructura del modelo está definida principalmente por las conexiones del sistema y sus cuatro elementos. En la tabla 2 se pueden identificar las particularidades de cada una de las interconexiones:

Tabla 2. Estructura del modelo de negocio de seguridad de la información

Interconexión	Características	Conexión	Finalidad	Consecuencias	Herramientas
Gobierno	Brinda las directrices a la empresa para su operación, con el fin de cumplir la estrategia (misión, visión y objetivo) dentro de los límites y controles establecidos por los procesos.	Estrategia y procesos	Tienen la finalidad de mantener el equilibrio del sistema, limitando los riesgos a niveles aceptables por la organización.	Una ineficiente gestión genera tensión en el sistema y falta de capacidad para adaptarse a situaciones emergentes.	Políticas, estándares y guías que demuestren que se cumplen los objetivos. Indicación de roles y responsabilidades, métricas de todo lo anterior y comunicación para mantener informados a todos los elementos del modelo.
Cultura	Patrón de comportamiento, creencias, presunciones, actitudes y formas de hacer las cosas.	Personas y estrategia	Entender la cultura para mejorar el programa de seguridad (qué se puede hacer, cómo hacerlo etc.).	Si no se conoce la cultura, difícilmente se puede fomentar la colaboración entre los elementos del modelo para adquirir conocimiento en lo referente a seguridad, acercar a las personas a dichos conceptos y comunicar eficientemente las decisiones.	Compuesta por la cultura organizacional (toda la empresa) y la cultura individual (personas).
Arquitectura	Base de un sistema que brinda organización al mismo	Estrategia y tecnología	Definir un diseño para preparar los planos y herramientas que transforman la visión /modelo en un producto real.	Si no se realiza la arquitectura del modelo, no se contaría con un espacio para la evolución y el mejoramiento. La arquitectura debe ser de fácil uso, apta para su propósito y consistente con las políticas y estándares.	Documentos, formatos políticas y estándares.
Habilitación y soporte	Se permite la realización de actividades (procesos) por medio de la tecnología que las apoya.	Procesos y tecnología	Contar con procesos estables y la tecnología capaz de soportar dichos procesos.	Si la solución tecnológica no es clara o es deficiente su definición, al igual que los requerimientos del negocio, se hace necesario revisar la estrategia y validar los requerimientos del servicio.	Objetivos de negocio de alto nivel, requerimientos del negocio, arquitectura de la empresa, macro procesos, planes y objetivos de la tecnología que se alineen con los planes y objetivos de la empresa.

Interconexión	Características	Conexión	Finalidad	Consecuencias	Herramientas
Surgimiento	Toda situación emergente que genera conocimiento para entender los requerimientos de seguridad y alinearloscon la estrategia	Personas y procesos	Ayuda en la personalización, mejora y amplía los procedimientos y normas de seguridad, llevando de la teoría a la práctica la seguridad de la información.	Puede ser clasificado como positivo o negativo. Positivo está relacionado con el proceso de aprendizaje para la comprensión de la seguridad, necesidades y mejoramiento de la seguridad de la información. Negativo está relacionado con el fenómeno creciente de la seguridad sin explicación de incidentes y la falta de alineación entre la seguridad de la información y los objetivos de negocio.	Procedimiento escrito: la ejecución de tareas basadas en el flujo específico de las acciones definidas. Políticas: la ejecución de tareas basadas en la política de la empresa. Ad-hoc: la ejecución de tareas de forma aleatoria; no están cubiertas por un procedimiento o una política.
Factores humanos	Interacción y/o brecha que existe entre las personas y la tecnología	Personas y tecnología	Identificar los factores humanos que afectan el programa de seguridad de la información, como lo son la edad, nivel de experiencia y expectativas frente al tema de seguridad.	Si las personas no entienden cómo utilizar la tecnología, existe algún rechazo hacia ella o no siguen las reglas para su uso, pueden existir amenazas de seguridad.	Diseño de tareas para involucrar a todos los miembros de la empresa en lo referente a seguridad, capacitación individual y grupal, selección de los individuos, diagnóstico para identificación de problemas, brechas entre la relación ser humanosistema.

Fuente: elaboración propia

2.4. Aplicaciones

Este modelo es aplicable a cualquier tipo de empresa y su éxito dependerá de los objetivos trazados por esta.

Para adoptar el modelo se deben seguir una serie de pasos. El primero consiste en analizar el entorno o contexto de la organización, lo que implica examinar la empresa según su ubicación geográfica, la relación con sus clientes externos e internos, proveedores, etc.

Una vez que los factores de negocio han sido identificados, las leyes y reglamentos aplicables se pueden integrar al programa de seguridad y al modelo. Luego, la empresa debe decidir qué otros referentes, buenas prácticas o modelos quiere aplicar para la gestión de seguridad y quién direcciona las reglas de gobierno o las directrices a adoptar. COBIT es un buen ejemplo de gobierno de TI.

Las soluciones existentes forman un patrón que se refleja tanto en los elementos como en las interconexiones. En este punto, se miden debilidades, fortalezas y se diseña un enfoque pragmático para identificar y cerrar brechas de seguridad que son visibles después de complementar el modelo. La forma circular de este da una clara visión sobre la manera de operar del sistema, las actividades que involucra y los comportamientos y patrones que se estabilizan con el tiempo, especialmente en lo referente a nivel de seguridad global de la empresa.

Referencias

ACIS. (Junio de 2017). *VII Jornada Nacional de Seguridad de la Información.* Bogotá, Colombia.

Canal, V. (Julio de 2010). A Revolution in Information Security: ISM Evolution with O-ISM3 [Mensaje en un blog]. Recuperado de https://www.slideshare.net/vaceituno/ism3-information-security-management-maturity-model

Canal, V. (2017). About O-ISM3 [Mensaje en un blog]. Recuperado de http://www.ism3.com/node/42

ISACA. (2009). *An Introduction to the Business Model for Information Security.* Rolling Meadows, IL.: ISACA. Recuperado de www.isaca.org/bmis: http://www.isaca.org/Knowledge-Center/BMIS/Documents/BMIS-22Sept2010-Research.pdf?regnum=412862

Kessinger, K. (6 de octubre de 2010). ISACA *Emite un Nuevo Modelo de NegocioComprensivo para la Seguridad deInformación*. Rolling Meadows, IL.: ISACA. Recuperado de https://www.isaca.org/About-ISACA/Press-room/News-Releases/Spanish/Pages/ISACA-Issues-Comprehensive-Business-Model-for-Information-Security-Spanish.aspx

The Open Group. (2017). *Open Information Security Management Maturity Model (O-ISM3), Version 2.0*.. Berkshire, United Kingdom: The Open Group Library. Recuperado de https://publications.opengroup.org/c17b

INFORMACIÓN TÉCNICA

FACULTAD DE
INGENIERÍA, DISEÑO
E INNOVACIÓN

Módulo: Teoría de la Seguridad

Unidad 2: Modelos de seguridad de la información

Escenario 4: Modelos modernos de seguridad de la información

Autor: Alexandra Peña Daza

Asesor Pedagógico: Angie Viviana Laitón Fandiño

Diseñador gráfico: Kelly Valencia

Asistente: Alejandra Morales