Gestiones de Seguridad de la Información en las Organizaciones

Cárdenas, Fabián. fabian.cardenas@novasec.co,

Resumen— En este contenido, se presenta una propuesta para visualizar y organizar de mejor manera un conjunto de actividades que permitan a las organizaciones controlar y dirigir sus acciones y decisiones con respecto a mejorar la seguridad de su información, para llegar finalmente a obtener un modelo de seguridad, coherente con la naturaleza del negocio y alineado con la norma ISO/IEC 27001, para lograr orientar con éxito la implementación de un SGSI[1].

Se presenta un conjunto de gestiones que deberían definir e implementar las empresas para ir avanzando en el nivel de completitud y madurez de su modelo de seguridad de la información, teniendo como base la gestión de:

- Los Activos de Información.
- Los Riesgos de SI[2].
- Los Incidentes de SI.
- El Cumplimiento.
- La Continuidad del Negocio.
- El Cambio y la Cultura Hacia la SI.
- La Estrategia de SI.

Para cada una de las gestiones se presenta su definición, la relación con cada una de las etapas del ciclo de mejora continua PHVA (Planear, Hacer, Verificar, Actuar) y la relaciones y dependencias que existen entre cada una de estas gestiones.

I. INTRODUCCIÓN

Los esfuerzos realizados por las organizaciones para afrontar la problemática de la seguridad de la información, con relación a los riesgos que conlleva la pérdida de su confidencialidad, integridad o disponibilidad, ha llevado a que las mismas aumenten cada año sus inversiones para minimizar en alguna proporción el nivel de su exposición al riesgo o el estado objetivo o subjetivo de inseguridad que perciban. Estas inversiones se traducen en proyectos que van desde una implementación tecnológica, que constituye un control de seguridad específico para la información, hasta proyectos tendientes a definir e implementar modelos de seguridad que permitan hacer una gestión continua de una estrategia de SI, que debe implementarse y mejorase a través del tiempo.

La norma internacional ISO/IEC 27001ha sido presentada al mundo, como un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de seguridad de la información, lo cual a priori nos indica que se puede generar un marco formal a través del cual se gestiona la seguridad de la información en las organizaciones. Es interesante ir a lo básico y preguntar: ¿Qué es la seguridad de la información? ¿que significa gestionar SI?.

La seguridad de la información es definida por la norma ISO/IEC 27001:2005 como: "La Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad"[6], de otra forma, y en un sentido práctico, como elemento de valor al negocio, puede definirse como: "La protección de la información contra una serie de amenazas para reducir el daño al negocio y maximizar las oportunidades y utilidades del mismo". Esta última definición nos sugiere con más fuerza que la seguridad de la información es un tema estratégico y de negocio que debe ser atendido desde la alta dirección.

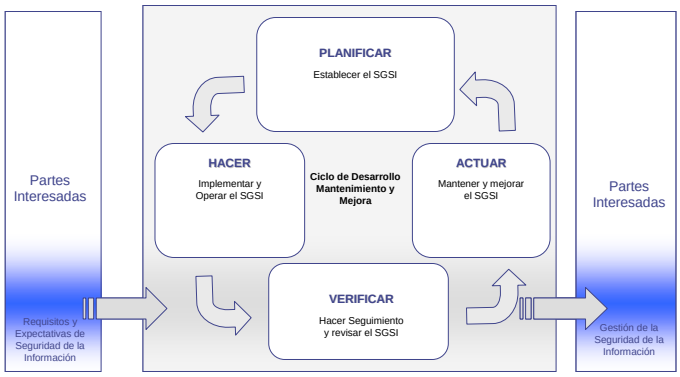
En este sentido gestionar es coordinar y dirigir una serie de actividades, con uno recursos disponibles, para conseguir determinados objetivos, lo cual implica amplias y fuertes interacciones

[1] SGSI: Sistema de Gestión de Seguridad de la Información. NTC ISO/IEC 27001:2005.
[2] SI: Seguridad de la Información

fundamentalmente entre el entorno, las estructuras, los procesos y los productos que se deseen obtener[3].

Teniendo en cuenta lo anterior, debemos reconocer que la gestión de la seguridad de la información requiere de una estrategia alineada con el negocio y sus objetivos, requiere de unos recursos y de un conjunto de actividades dirigidas y coordinadas por una organización de la seguridad que se extienda a través de toda la organización, desde la alta dirección hasta los usuarios finales.

En el desarrollo de este artículo se presenta cual es ese conjunto de actividades principales que deben llevarse a cabo dentro de una gestión de seguridad de la información, en la cual existe un marco general que es el ciclo de mejora continua PHVA, bajo el cual se orquestan varias gestiones que alineadas completan y soportan los objetivos de seguridad de la información que normalmente se buscan satisfacer en las organizaciones.



En este sentido es importante ir más allá de tener unos requisitos normativos y de conformidad con un estándar internacional y presentar los elementos prácticos que permitan que las organizaciones comprendan y dimensionen los esfuerzos que hay que llevar a cabo para gestionar la seguridad de la información de manera sistemática.

II. GESTIONES DE SEGURIDAD DE LA INFORMACIÓN

A. Gestión de Activos de Información

Definición

En esta gestión se requiere identificar, valorar y clasificar los activos de información más importantes del negocio. Un activo de información en el contexto de un SGSI y con base en la norma ISO/IEC 27001:2005 es: "algo a lo que una organización directamente le asigna un valor y por lo tanto la organización debe proteger" [6].

Para las organizaciones esta definición de activo de información puede resultar muy amplia, por lo cual es necesario establecer unos criterios qué permitan identificar lo que es un activo de información y definir las distintas formas en las cuales se pueden reconocer estos en la organización.

Se debe considerar como un activo de información principalmente a cualquier conjunto de datos[4] creado o utilizado por un proceso de la organización., así como el hardware y el software utilizado para su procesamiento o almacenamiento, los servicios utilizados para su transmisión o recepción y las herramientas y/o utilidades para el desarrollo y soporte de sistemas de información. En casos particulares, se puede considerar como un activo de información a personas que manejen datos, transacciones, o un conocimiento especifico muy importante para la organización (Por ejemplo: secretos industriales, manejo de claves importantes, know how)

Bajo esta gestión se persigue dar cumplimiento a tres puntos principales:

1) Inventario de Activos: Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de todos los activos de información importantes de la organización.[6]

Este inventario debe tener la valoración de cada activo, indicando bajo una escala definida por la organización, por ejemplo, si es de alto, medio, o bajo valor. Adicionalmente es importante que se indique cuales son las propiedades más importantes de proteger para cada activo en términos de su CID[5], valorando cada propiedad. Se debe indicar

[3] Adaptado de [4]

[4] Dato: Unidad mínima que compone cualquier información, por lo cual la información finalmente debe considerarse un conjunto organizado de datos que tiene sentido y valor para la organización.

[5] CID: Confidencialidad, Integridad y Disponibilidad.

cual es la ubicación del activo de información y cuales son los procesos que lo utilizan.

2) Propiedad de los Activos: Toda la información y los activos asociados con los servicios de procesamiento de información deben ser "propiedad"[6] de una parte designada de la organización [6]. En este sentido se puede determinar algunos entes que interactúan con los activos de información como lo son:

Propietario de la Información: El cual es una parte designada de la organización, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de definir quienes tienen acceso, que pueden hacer con la información, y de determinar cuales son los requisitos para que la misma se salvaguarde ante accesos no autorizados, modificación, pérdida de la confidencialidad o destrucción deliberada y al mismo tiempo de definir que se hace con la información una vez ya no sea requerida, así como los tiempos de retención asociados a la misma.

Custodio Técnico: Es una parte designada de la organización, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad (Toma de copias de seguridad, asignar privilegios de: Acceso, Modificaciones, Borrado) que el propietario de la información haya definido, con base en los controles de seguridad y recursos disponibles en la organización.

Usuario: Cualquier persona que genere, obtenga, transforme, conserve o utilice información de la organización en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la organización. Son las personas u otros sistemas que utilizan la información para propósitos propios de su labor, y que tendrán el derecho manifiesto de su uso dentro del inventario de información. Para cada usuario se debería definir los derechos y niveles de acceso al activo de información (lectura, escritura, borrado, entre otros.).

[6] El término "Propietario" identifica a un individuo o a una entidad que tiene responsabilidad aprobada de la dirección por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos. El término "Propietario" no implica que la persona tenga realmente los derechos de propiedad de los activos.[6]

3) Directrices de Clasificación: La información debe clasificarse en términos de su valor, de los requisitos legales, de su sensibilidad y la importancia para la organización.[6]

Los niveles de clasificación de la información para cada organización pueden variar de alguna forma, y normalmente se establecen en términos de su confidencialidad, aunque puede establecerse un esquema tan completo que abarque niveles de clasificación por características de disponibilidad e integridad. Un esquema sencillo de clasificación, en términos de confidencialidad, puede manejar dos niveles, por ejemplo, información pública e información confidencial. Para otras organizaciones dos niveles pueden ser no suficientes y en cambio puede existir información: pública, de uso interno, confidencial y altamente confidencial.

En cualquier caso la organización deberá definir que significa cada uno de esos niveles y los grados de discreción necesarios para traducirlos a que se implemente un tratamiento y manejo seguro de la misma para cada uno de los niveles de clasificación definidos, esto como mínimo en cuanto:

- Los niveles de acceso permitidos.
- Los métodos de distribución y/o transmisión.
- Condiciones de almacenamiento.
- Condiciones de entrega de terceros.
- Destrucción.

En este punto, el tema de manejo y tratamiento se establece con base en mejores prácticas de seguridad, que pueden ser aplicadas para cada nivel de clasificación de manera general para todos los activos de dicho nivel. Si se requiere un nivel de tratamiento y manejo particular para un activo de información, esto deberá responder y justificarse a través de la identificación de un riesgo específico sobre dicho activo, en la Gestión de Riesgos.

Principales Actividades en el Ciclo de Mejora Continua PHVA

Planear:

- Definir que es un activo de información para la organización.
- Establecer un método de identificación y valoración de activos de información.
- Definir un esquema de clasificación.
- Establecer el tratamiento y manejo para los activos de información en cada nivel de clasificación establecido.

Hacer:

- Levantar la información de los activos de información utilizados en los procesos de la organización.
- Identificar y valorar los activos de información.
- Clasificar los activos de información.
- Hacer parte de las actividades del día a día, en los procesos de la organización, el tratamiento y manejo definido para cada nivel de clasificación.

Verificar:

- Revisar las valoraciones realizadas a los activos de información si ocurren cambios en el negocio o en la tecnología.
- Hacer una revisión de la calidad de la información consignada en el inventario.
- Realizar auditorías de cumplimiento del tratamiento y manejo de acuerdo a los niveles de clasificación estipulados.

Actuar:

- Realizar actualizaciones en la información del inventario de activos.
- Adelantar las recomendaciones producto de las auditorías realizadas.

Algunas Relaciones y/o Dependencias

- La gestión de activos de información es un prerrequisito para la gestión de riesgos de seguridad de la información.
- Cada vez que se reconozca un nuevo activo de información o se genere un cambio en alguno existente se deberá realizar una revisión del riesgo para dicho activo.
- Los incidentes de seguridad de la información se generan sobre uno o más activos de información del negocio.
- Los activos de mucho valor para el negocio, que posean necesidad de un alto grado de disponibilidad, normalmente están en el alcance de la gestión de la continuidad del negocio.

B. Gestión de Riesgos de Seguridad de la Información

Definición

Esta gestión es un conjunto de actividades para controlar y dirigir la identificación y administración de los riesgos de seguridad de la información, para así poder alcanzar los objetivos del negocio. El riesgo es una característica de la vida de los negocios por lo cual hay que tener un control sobre los mismos.

La gestión de riesgos de SI debe garantizar que el impacto de las amenazas que podrían explotar las vulnerabilidades de la organización, en cuanto a la seguridad de su información, estén dentro de los límites y costos aceptables.

Aunque la naturaleza del negocio de cada organización puede ser diferente, o tener variaciones que hacen que los riesgos sean distintos, es importante que la organización, independiente de la metodología de identificación, evaluación y tratamiento de riesgos que seleccione, tenga en cuenta el manejo de los siguientes elementos para la gestión de riesgos de seguridad de la información.

Vulnerabilidad: Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos de una organización.

Amenaza: Es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la organización.

Riesgo: Es la definición de un escenario bajo el cual una amenaza puede explotar una vulnerabilidad, generando un impacto negativo al negocio (por ejemplo, pérdida de la continuidad, incumplimiento, pérdida de ingresos, entre otros).

Probabilidad: Es una cuantificación para determinar en que nivel un hecho o acontecimiento pueda producirse. En este caso aplicado a la probabilidad de que una amenaza explote una vulnerabilidad para que se produzca o se materialice un riesgo.

Impacto: Es un efecto que ocurre a causa de la materialización de un riesgo y que va en detrimento de uno o más de los recursos importantes del negocio (Recursos: Financiero, Imagen, Ambiental, Humano, entre otros).

Tratamiento: Es el conjunto de acciones que debe desarrollar la organización para poder bajar el nivel de exposición al riesgo, a través de la disminución de la probabilidad o del impacto, o por ejemplo, cesar la actividad que de origen al riesgo en un caso muy extremo. Comúnmente el tratamiento se realiza a través de la implementación de controles de seguridad de la información.

Riesgo Puro: Es el nivel de impacto ante el riesgo que existe antes de aplicar cualquier acción de tratamiento.

Riesgo Residual: Es el nivel de impacto ante el riesgo que persiste después de aplicar cualquier acción de tratamiento. El riesgo residual siempre deberá ser menor que el riesgo puro.

La gestión de riesgos de SI representa una de las labores más dispendiosas, pero al mismo tiempo más importantes, dentro del modelo de implementación de un SGSI. Lo anterior se indica dado que las actividades recomendadas a realizar como mínimo son:

- Identificación: Identificar vulnerabilidades y amenazas para cada activo de información y describir el riesgo inherente.
- Evaluación: Establecer la probabilidad de ocurrencia del riesgo e identificar el impacto sobre los recursos del negocio, en términos de CID para cada recurso si es posible.
- Tratamiento: Identificar los controles de seguridad a nivel tecnológico, procedimiental o del talento humano existentes, o los nuevos que sean necesarios, para llevar los riesgos a los niveles residuales aceptables para el negocio, teniendo en cuenta una priorización de los riesgos que generan un mayor impacto. Para este tratamiento se utiliza como referencia la norma ISO/IEC 17799:2005, de la cual se pueden seleccionar los objetivos de control y los controles de seguridad a implementar, los cuales están debidamente tipificados en 11 dominios o áreas de trabajo.
- Monitoreo: Revisar periódicamente si las condiciones cambiantes de la organización pueden sugerir cambios en la información definida para la identificación y evaluación de los riesgos.
- Comunicación: Informar a los diferentes niveles de la organización y a los interesados en la gestión de riesgos, acerca de las acciones realizadas y los planes de tratamiento a ejecutar para asegurar los recursos necesarios para las tareas a llevar a cabo.

En el proceso de gestión de riesgos las decisiones más importantes tienen que ver con el tratamiento que se determine para cada riesgo, mediante un esfuerzo continuo de llevar los riesgos a unos niveles aceptables, bajo un esquema de costo-beneficio para la organización.

Principales Actividades en el Ciclo de Mejora Continua PHVA

Planear:

- Definir la metodología para la identificación, evaluación y tratamiento del riesgo.
- Establecer los recursos del negocio sobre los cuales de medirán los impactos.
- Establecer los criterios para definir los niveles de riesgos aceptables.
- Identificar la manera como se desplegarán y ejecutaran los planes de acción para el tratamiento de los riesgos.

Hacer:

- Identificar vulnerabilidades, amenazas y riesgos de SI.
- Determinar la probabilidad de ocurrencia del riesgo
- Determinar el impacto al negocio sobre sus recursos del mismo.
- Definir los planes de tratamiento de riesgo.

Verificar:

- Monitorear si se realizan nuevas evaluaciones de riesgos con base en los cambios en el negocio.
- Hacer seguimiento a la implementación de los planes de acción para el tratamiento de los riesgos.
- Revisar si los niveles de riesgos son aceptables o no.

Actuar:

- Realizar actualizaciones en la evaluación de riesgos existentes.
- Determinar acciones de mejora para las desviaciones que se presenten en el despliegue de los planes de acción para el tratamiento de los riesgos.

Algunas Relaciones y/o Dependencias

- La gestión de activos de información es uno de los principales insumos de esta gestión. Adicionalmente, aunque no se presentan como gestiones sino como actividades de SI, las pruebas de vulnerabilidades e intrusión lógica y física, los diagnósticos de capacidad de la infraestructura de TI y los diagnósticos de cumplimiento con normas y estándares de seguridad, son insumos para determinar amenazas, vulnerabilidades e impactos para la gestión de riesgos.
- Cada vez que se suscite un incidente de SI se debe revisar y evaluar las amenazas y vulnerabilidades de los activos de información que estuvieron involucrados, para verificar si se tienen ya evaluados o no los elementos que se identificaron y analizaron como causas del incidente de SI.
- Algunos riesgos de seguridad identificados generan la necesidad de tratamiento a través de planes de continuidad del negocio (entrada a la gestión de a continuidad del negocio).
- La gestión del cambio y la cultura de SI debe ser un instrumento a través de cual se comunique a la organización la importancia de la SI para mitigar los riesgos identificados e esta gestión.
- La gestión de riesgo, en su etapa de tratamiento, genera una serie de planes y proyectos a corto, mediano y largo plazo y a diferentes niveles, a los cuales se les debe hacer seguimiento a través de la gestión de la estrategia de SI.

C. Gestión de Incidentes de Seguridad de la Información

Definición

Para comprender el objetivo de esta gestión hay que recurrir a las siguientes definiciones base:

Evento de seguridad de la información: un evento de seguridad de la información es la presencia identificada de un estado que indica un incumplimiento posible de la política de seguridad de la información, una falla de los controles de seguridad, o una situación desconocida que puede ser pertinente para la seguridad de la información.

Incidente de seguridad de la información: un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de los activos de información.

Los incidentes de seguridad de la información son hechos inevitables sobre cualquier ambiente de

información, y estos pueden ser bastante notorios e involucrar un impacto fuerte sobre la información de la organización.

Existe una gran cantidad de métodos para afrontar los incidentes, pero si no se está preparado adecuadamente para la gestión de los mismos es muy probable que no se manejen correctamente y dentro de los tiempos necesarios, impidiendo adicionalmente que se pueda aprender de la ocurrencia y el atención de los mismos.

El objetivo principal de la Gestión de incidentes es definir un proceso que permita manejar adecuadamente los incidentes a través de un esquema que involucra las siguientes actividades de manera cíclica:

- Preparación para la gestión de Incidentes: En la preparación se debe procurar por obtener los recursos de atención de incidentes y las herramientas necesarias para los demás procesos del ciclo de vida. Se deben validar los procedimientos existentes, programas de capacitación y propender por la mejora de los mismos de ser necesario. La preparación también involucra un componente de prevención de Incidentes.
- Detección y análisis: La fase de detección y análisis se puede descomponer en dos elementos:

  Clasificación de incidentes de acuerdo a la política y a las revisiones de esta clasificación con base en la experiencia generada por los incidentes ocurridos.

  Identificación y gestión de elementos Indicadores de un incidente, los indicadores son los eventos que nos señalan que posiblemente un incidente ha ocurrido.

- Contención, Erradicación y Recuperación: Se deben establecer mecanismos para evitar que el incidente se propague y pueda generar mas daños a través de toda la infraestructura, para lograr esto se debe definir una estrategia de contención. En este proceso se elimina cualquier rastro dejado pro el incidente, por ejemplo código malicioso, y posteriormente se procede a la recuperación a través de la restauración de los servicios afectados usando procedimientos de recuperación y quizás de continuidad.
- Actividades post incidente: Las actividades Post-Incidente básicamente se componen del reporte apropiado del incidente, de la generación de lecciones aprendidas, del establecimiento de medidas disciplinarias y penales de ser necesarias y el registro en la base de conocimiento para alimentar indicadores de gestión del SGSI.

Adicionalmente la organización debe reconocer cuales son los tipos de incidentes que debe identificar y manejar, determinando los diferentes niveles de severidad para así determinar el tratamiento adecuado a cada uno de estos en cada una de las actividades antes descritas.

La norma NTC-ISO/IEC 27001:2005 entrega unos lineamientos a tener en cuenta a la hora de establecer la Gestión de los incidentes de seguridad, definiendo unos controles necesarios para dar cumplimiento a estos lineamientos.

La Norma plantea los siguientes puntos a desarrollar sobre la gestión de incidentes:

- Reporte sobre los eventos y las debilidades de la seguridad de la información.
  - Reporte sobre los eventos de seguridad de la información
  - Reporte sobre las debilidades en la seguridad
- Gestión de los incidentes y las mejoras en la seguridad de la información
  - Responsabilidades y procedimientos
  - Aprendizaje debido a los incidentes de seguridad de la información
  - Recolección de evidencias.

Si se está manejando un modelo de seguridad de conformidad con la norma ISO/IEC 27001:2005 se

deberán entonces incluir estos elementos dentro de las cuatro actividades anteriormente planteadas.

Principales Actividades en el Ciclo de Mejora Continua PHVA

Planear:

- Preparación para la gestión de incidentes.
- Definición de los procedimientos de Detección y análisis, Contención, Erradicación y Recuperación.
- Clasificación de los incidentes y su grado de severidad.
- Definición de los elementos indicadores de un incidente.

Hacer:

- Detectar y analizar incidentes.
- Contener, Erradicar y Recuperarse de un incidente
- Comunicar y escalar los incidentes.
- Documentar los incidentes de seguridad.

Verificar:

- Pruebas y auditorías a los procedimientos de atención de incidentes.

Actuar:

- Definir acciones preventivas y correctivas con base en los incidentes ocurridos.

Algunas Relaciones y/o Dependencias

- Un incidente de SI debe ser analizado adicionalmente para determinar su connotación de responsabilidad penal y civil, para que de esta forma la disminución de los nuevos riesgos identificados y las actuaciones requeridas se administren en la gestión del cumplimiento.
- Los incidentes de seguridad deben comunicarse para que la organización aprenda de los mismos y no vuelvan a ocurrir. En este sentido debe incluirse el manejo de lecciones aprendidas en las comunicaciones y capacitaciones realizadas en la gestión del cambio y cultura en SI.
- Un incidente de seguridad puede dar lugar a la identificación de nuevos riesgos de seguridad de la información.
- Los procedimientos de contención, erradicación y recuperación ante incidentes deben estar alineados con los planes de continuidad del negocio.
- Ciertos incidentes de seguridad deben estar formalmente tipificados, de tal forma que cuando se presenten sean el elemento disparador de la declaración formal de la ejecución de un plan de continuidad de negocio.

D. Gestión del Cumplimiento

Esta gestión permite identificar y administrar los riesgos de carácter jurídico que puede afrontar la organización, con respecto a incidentes presentados sobre sus activos de información, que se puede generar sobre diferentes componentes como son: comercio electrónico, protección de datos, habeas data, los incidentes informáticos y su connotación en términos de responsabilidad penal y civil, contratación informática y telemática, contratación laboral, contratación con terceros, derecho a la intimidad, la legislación propia del sector o industria, entre otros.
Lo que se busca es que se identifiquen los posibles riesgos que no han sido atendidos en las áreas legales antes mencionadas y para lo cual la empresa se podría encontrar vulnerable y a través de esta gestión atenderlos.

Esta gestión aunque es muy parecida a la gestión de riesgos de seguridad de la información, en algunas ocasiones puede no tener la misma naturaleza ni atenderse a través de los mismos métodos para la identificación y evaluación de los riesgos. En algunos casos por que la identificación y evaluación no se realiza por cada activo de información sino se determina un nivel de exposición al riesgo general de la organización, dado que son temas transversales a la organización, y en otras ocasiones por que es difícil de cuantificar el impacto sobre todos los recursos del negocio y no aplicarían las escalas determinadas de impacto sino que se manejarían elemento más generales.

Con esta gestión se aborda la seguridad de la información desde el ámbito jurídico, y por ende el tratamiento se realiza a través de controles jurídicos con base en la ley del país, o los que apliquen a nivel internacional, o en un caso específico al

negocio por parte de un ente regulador o de control, y los reglamentos internos disciplinarios y de trabajo.

Principales Actividades en el Ciclo de Mejora Continua PHVA

Planear:

- Estudiar las áreas legales que apliquen y que puedan generar riesgos a la organización y determinar como se abordaría su identificación, evaluación y tratamiento.

Hacer:

- Identificar y evaluar los riesgos de cumplimiento y definir su tratamiento.
- Implementar los controles jurídicos indicados en el tratamiento.

Verificar:

- Revisar los controles jurídicos establecidos para determinar si siguen siendo suficientes de acuerdo a cambios que se susciten en el negocio o el entorno jurídico nacional e internacional.

Actuar:

- Realizar las acciones de cambio o mejora a los controles jurídicos establecidos.

Algunas Relaciones y/o Dependencias

- La gestión de riesgos de SI puede ser utilizada como una entrada para la gestión de cumplimiento, en cuanto a identificar ciertos activos de información que presenten riesgos que puedan generar un impacto importante sobre las áreas legales.
- La clasificación de los incidentes permite identificar las actuaciones que a nivel legal se tendrían que llevar a cabo al momento de presentarse un incidente de SI, principalmente en la etapa post incidente.
- Los controles jurídicos a implementar para el tratamiento de riesgos de incumplimiento generan cambios o proyectos a los cuales se les tiene que hacer seguimiento en la gestión de la estrategia de SI.

E. Gestión de la Continuidad del Negocio

Esta gestión desarrolla y administra una capacidad para responder ante incidentes destructivos y perjudiciales relacionados con la seguridad de la información que impidan continuar con las funciones y operaciones críticas del negocio, además debe tender por la recuperación de estos escenarios tan rápida y eficazmente como se requiera. Esta gestión debe permitir reducir el riesgo comercial y operacional de la organización.

Esta gestión tiene como actividades principales las siguientes:

- Realizar un análisis de impacto al negocio (BIA).
- Identificar y priorizar los recursos que soportan la actividad de los procesos de la organización.
- Elegir las estrategias apropiadas de recuperación.
- Elaborar planes de recuperación (DRP).
- Desarrollar planes de continuidad para la funciones críticas del negocio (BCP).
- Capacitar al personal en la ejecución y mantenimiento de los planes.
- Revisar y mantener los planes por cambio en el negocio o en la infraestructura.
- Almacenar de manera segura los planes y contar con medios alternos de comunicación.
- Probar y auditar los planes.

Dentro de esta gestión se tiene que tener en cuenta que los objetivos principales son: Mantener las funciones críticas del negocio en los niveles aceptables que generen las menores pérdidas posibles, recuperarse rápida y eficazmente, minimizar el impacto generado por la pérdida de la continuidad, responder en forma sistemática, aprender y ajustar los planes para reducir la probabilidad de que el incidente vuelva a ocurrir, resolver posibles problemas legales y operativos que se puedan suscitar y que no hayan sido previstos en el BIA.

De los elementos mínimos a tener en cuenta en las estrategias de recuperación y continuidad están:

- Las máximas ventanas de interrupción.

- Los objetivos de tiempo de recuperación (RTO, tiempos máximo tolerado para la recuperación).
- Objetivos de punto de recuperación (RPO, máxima antigüedad de los datos tolerada una vez recuperada la continuidad).
- Objetivos de entrega de servicio (SDO, niveles de servicio que se tienen que soportar mientras persiste la eventualidad)
- El máximo tiempo de funcionamiento en modo alterno o de contingencia.

Esta gestión debe responder a la necesidad de continuidad para riesgos de seguridad identificados que impacten principalmente la disponibilidad de los activos de información, y además que de respuesta a la protección ante incumplimientos de niveles de servicios y cláusulas contractuales, que puedan generar un detrimento principalmente en los recursos financieros y de imagen en las relaciones con socios de negocio, proveedores y clientes.

Principales Actividades en el Ciclo de Mejora Continua PHVA

Planear:
- Definir la metodología y los recursos del negocio que van a ser analizados en el BIA.
- Definir los objetivos de continuidad y recuperación.

Hacer:
- Desarrollar e implementar los planes de continuidad y recuperación.
- Capacitar al personal en la ejecución y mantenimiento de los planes.
- Diseñar e implementar la infraestructura de TI y de procesos que dará soporte a la ejecución de los planes.

Verificar:
- Revisar y mantener los planes por cambio en el negocio o en la infraestructura.
- Realizar pruebas y auditorías a los planes de continuidad y recuperación.

Actuar:
- Actualizar los planes de continuidad y recuperación.
- Reforzar debilidades detectadas en las pruebas y auditorias.

Algunas Relaciones y/o Dependencias

- La gestión de la continuidad del negocio debe responder a la necesidad de mitigación de varios riesgos de SI que pueden afectar varios activos de información del negocio.
- Algunos riesgos identificados en la gestión del cumplimiento generan la necesidad de contar con planes de continuidad sobre ciertos funciones críticas del negocio que ciertos entes reguladores del sector exigen.
- La gestión de riesgos de SI puede ser utilizado como un insumo muy importante para identificar los riesgos asociados con la pérdida de la continuidad del negocio y así establecer un panorama más completo de perdida de continuidad en el BIA.

F. Gestión del Cambio y la Cultura hacia la SI

Esta gestión se enfoca a lograr un nivel alto de compromiso y actuación de todos los integrantes de la organización en el SGSI como parte fundamental del sistema. Esta gestión se convierte en un medio de vital importancia para difundir la estrategia de seguridad de la información a los diferentes niveles de la organización, para generar un cambio positivo hacia los nuevos papeles que entrarán a jugar las personas en la protección de los activos de información del negocio. El hecho de no tener un nivel adecuado de sensibilización en SI deja en una situación de riesgo a la organización.

La cultura en SI debería buscarse con base en la siguiente definición: “Es el conjunto de presunciones básicas que desarrolla un grupo dado, a medida que va aprendiendo a enfrentarse con sus problemas de adaptación externa e integración interna, y que han ejercido la suficiente influencia como para que puedan considerarse válidas y en consecuencia puedan enseñarse a los nuevos miembros de una organización, como el modo correcto de percibir, pensar, sentir y actuar y que estos puedan reforzarlos.”[2]

Como parte de esta gestión se realizan las siguientes actividades básicas:

- Establecer los diferentes grupos objetivos que puedan existir y definir una estrategia

para las actividades de gestión del cambio y la comunicación que debe llegar a cada grupo, si es posible, con base en los niveles de resistencia al cambio observados históricamente y utilizando a los líderes y stakeholders que puedan influenciar de manera positiva el desarrollo de las actividades planteadas.[3]

- Definir las herramientas y medios a través de los cuales se desplegará la estrategia de gestión de cambio.
- Comunicar la estrategia de SI y las mejores prácticas y hábitos de comportamiento que son importantes para poder obtener un nivel adecuado de protección de los activos de información.
- Definir los planes de capacitación requeridos para generar las competencias necesarias en el personal, para que lleven a cabo las actividades de seguridad de la información que sean desplegadas hacia sus procesos y que se interiorice la importancia de la SI.
- Realizar una medición periódica de la efectividad de los planes desarrollados y de los niveles de aprendizaje y comportamiento de las personas, para en caso de falencias establecer cambios y mejoras en la estrategia.

Principales Actividades en el Ciclo de Mejora Continua PHVA

Planear:

- Establecer una estrategia de gestión de cambio y formación de cultura de SI..

Hacer:

- Desarrollar los planes y programas de gestión de cambio y sensibilización en SI.
- Desarrollar los planes de capacitación.

Verificar:

- Revisar y medir periódicamente la efectividad de los planes implementados.

Actuar:

- Realizar las acciones de cambio o mejora a los planes de gestión de cambio y capacitación.

Algunas Relaciones y/o Dependencias

- La gestión del cambio debe comunicar de la mejor manera a la organización la estrategia de SI y el panorama de riesgos de SI y sus impactos a la organización y principalmente sobre el recurso humano.
- Los planes de capacitación definidos en esta gestión deben estar alineados con los planes y proyectos de tratamiento de riesgos para que las personas estén preparadas para hacer uso de nuevas tecnologías, procedimientos o tener nuevas actuaciones con respecto a la SI.
- La gestión del cambio y cultura en seguridad debe ser una de las primeras en realizarse en el SGSI, y debe ser lo suficientemente exitosa para que todas las demás gestiones se soporten en la buena actuación y compromiso del recurso humano, con respecto a las actividades que hay que desplegar a través de toda la organización.

G. Gestión de la Estrategia de SI

Para poder controlar y dirigir todas estas gestiones se hace necesario que la organización despliegue las mismas desde el más alto nivel de la organización, a través de:

Declaraciones Formales de Intención y Compromiso: Estas se materializan a través de políticas organizacionales que la alta dirección presenta a la organización (Por ejemplo: Política de SI, Política del SGSI o de la Información). Estas declaraciones podría estas conformada por una general y una para cada gestión de seguridad. Todos los demás niveles de documentación relacionados con la SI a través de la organización, (Normas, Procedimientos, guías, etc) deben estar alineados y deben apoyar estas declaraciones de alto nivel, para que las mismas sean operativas y coherentes a través de las diferentes gestiones de seguridad.

De esta declaración y compromiso también hace parte el alcance que la alta dirección se compromete a tener dentro de la gestión, la cual puede hacerse solo para los procesos más importantes y para los activos del negocio de mayor valor inicialmente, teniendo una visión de implementación incremental a través del tiempo en donde dicho alcance puede

aumentar progresivamente, lo cual es lo recomendado.

Definición de Roles, Responsabilidades y Recursos: Se debe definir quien y con que recursos se ejecutarán las diferentes actividades del ciclo PHVA de cada una de las gestiones. Más que preocuparse inicialmente por una estructura organizacional (Unidad, Área o Dirección) lo que se debe definir es a través de la organización quien tiene que responsabilidades en los diferentes niveles, desde la alta dirección hasta los usuarios finales.
Una estructura organizacional específica puede quedar muy limitada al momento de asignársele algunas responsabilidades que en realidad deben estar sobre las personas que ejecutan los procesos de la organización, para que las actividades de seguridad hagan parte del día a día y se desplieguen y se apropien en las personas.
Un área de seguridad de la información deberá estar orientada a orquestar y dirigir estas gestiones y poder enmarcarlas dentro del SGSI de manera integral.

Medición y Control: Los resultados de los esfuerzos realizados y el estado de la seguridad de la información debe incluirse en los mecanismos y herramientas de apoyo a la toma de decisiones de la organización. Por esta razón es importante que cada gestión posea indicadores de desempeño de sus actividades más representativas, y que estos a su vez representen un nivel de indicadores que están alineados con los indicadores de mayor nivel, que hacen posible el logro de los objetivos corporativos.
Es necesario que se utilicen herramientas de medición y control mediante cuadros de mando gerenciales y metodologías para su despliegue y organización (por ejemplo: Un BSC – Balanced Scorecard).

Modelo de gobierno de la Seguridad de la Información: Se busca que la estrategia de seguridad de la información tenga un marco de gestión formal, lo cual puede establecerse a través de la decisión organizacional de estar en conformidad o cumplimiento con uno o más modelos ampliamente aceptados mundialmente. La escogencia de dicho marco dependerá del tipo de organización, su tamaño, sus objetivos de seguridad y del alcance, nivel de madurez y completitud la cual quieran llegar en el tema de seguridad de la información. Algunos de estos marcos o modelos que apoyan la gestión y que en la mayoría de los casos se complementan y comparten recursos son: COBIT, ISO/IEC 27001:2005, ISO/IEC 17799:2005, ISO 9001:2000, ISM3, ITIL, entre otros.

Finalmente estos marcos o modelos influenciarán la manera como se desplieguen las diferentes gestiones aquí presentadas, en este artículo los elementos presentados aunque de manera genérica, están orientados a la conformidad con la norma ISO/IEC 27001:2005.

Principales Actividades en el Ciclo de Mejora Continua PHVA

Las actividades de esta gestión se dan en un mayor nivel, ya que de manera general integra a las demás gestiones estableciendo el marco de gestión estratégico del SGSI.

Planear:
- Definir la estrategia y políticas de SI.
- Definir la organización de la seguridad.
- Definir los objetivos de la seguridad de la información.
- Definir los indicadores de gestión y la metodología de despliegue y medición.
- Definir el alcance del SGSI.

Hacer:
- Comunicar y establecer la estrategia de SI.
- Medir los indicadores definidos.
- Implementar las acciones que conlleven a desplegar las diferentes gestiones de seguridad de la información. En el SGSI

Verificar:
- Hacer seguimiento a los planes de implementación de las diferentes gestiones de SI del SGSI.
- Revisar los productos y resultado de las pruebas y auditorías que deben generarse a partir de las diferentes gestiones.
- Revisar el resultado de las diferentes gestiones con base en los indicadores de SI.

Actuar:

- Ejecutar las acciones preventivas y correctivas generadas en las diferentes gestiones de seguridad..

Es importante que no se pierda de vista que una gestión puede haber realizado el cierre del ciclo PHVA una o más veces, mientras que una gestión "más joven" apenas esté en la mitad de su primer ciclo (gestión planeada y en implementación), lo cual nos ayuda a entender precisamente el concepto de mejora continua, en el sentido en que las diferentes gestiones van madurando y completándose a través del tiempo, hasta que el SGSI es más "fácil" de operar y mantener.

III. CONCLUSIONES

La gestión de la seguridad basada en modelos tan completos y a la vez complejos representan un reto en cuanto a la implementación para las organizaciones, las cuales deben entender las implicaciones y el nivel de esfuerzo requerido, para lo cual se debe planificar muy bien para llegar a tener una estrategia de implementación exitosa.

Las normas de seguridad de la información nos indican comúnmente los elementos del "que hacer" o el "debe hacer", pero en su gran mayoría no es de su alcance el "cómo hacerlo" o el "así se hace". A pesar de que se están haciendo esfuerzos por acompañar estas normas con guías de implementación, para nuestras organizaciones generará mayor valor el compartir las experiencias reales de implementación de las compañías y el "cómo" de vencer ciertos retos en la definición e implementación de un SGSI.

La implementación de Sistemas de Gestión de Seguridad de la Información debe ser una iniciativa de debida diligencia de la alta dirección de las organizaciones, bajo el cual se gestionará la seguridad de la información para convivir de la mejor manera con los riesgos inherentes a la naturaleza de cualquier negocio.

REFERENCIAS

[1] Calder. Alan, Nueve Claves para el Éxito, una visión de la implementación de la norma NTC-ISO/IEC 27001, ICONTEC, 2006, pp. 13-38.

[2] Glosario Institucional, Policía Nacional de Colombia, www.policia.gov.co/inicio/portal/portal.nsf/paginas/GlosarioInstitucional.

[3] Jones. John. 10 Principles of Change Management, tools and techniques to help companies transform quickly, 2004, pp. 1-4.

[4] Marecos. Edgardo, Conceptos Claves Acerca de la Salud, Revista de Postgrado de la Cátedra VIa Medicina, 2001, pp. 17-19.

[5] ISACA, Manual de Preparación del Examen CISM, 2005, pp. 53-82, 186-225.

[6] NTC-ISO/IEC 27001:2005, ICONTEC, 2006.

Autor

Fabián Alberto Cárdenas Varela