SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL CLUB MILITAR DESDE LA NORMA ISO 27001:2005

LUIS ALBERTO LÓPEZ CASTAÑO

UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD DE CIENCIAS ECONÓMICAS
PROGRAMA ESPECIALIZACIÓN EN CONTROL INTERNO
BOGOTA OCTUBRE 26-2013

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL CLUB MILITAR DESDE LA NORMA ISO 27001:2005

LUIS ALBERTO LÓPEZ CASTAÑO

LUZ MERY GUEVARA CHACÓN
ASESORA

UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD DE CIENCIAS ECONÓMICA
PROGRAMA ESPECIALIZACIÓN EN CONTROL INTERNO
BOGOTA OCTUBRE 26-2013

LISTA DE CUADROS.

INTRODUCCIÓN

El Club Militar es una entidad adscrita al Ministerio de la Defensa Nacional, de carácter público con patrimonio propio y autonomía administrativa, con el objetivo misional de proporcionar servicios con calidad en bienestar y recreación, que permitan la plena satisfacción y desarrollo integral de los oficiales activos y de la reserva activa de la fuerza pública y sus familias. Para el desarrollo de una parte de lo misional se apoya en la tecnología de la información y las comunicaciones las cuales se administran y protegen desde el departamento de sistemas de la organización.

A continuación se hace una breve descripción de la problemática actual del Club Militar, referente a la protección de los inventarios de activos de datos, los cuales a la fecha no están actualizados, siendo éstos los de mayor importancia, pues son los que contienen los registros que se generan en las operaciones misionales que están de frente al socio denominado front office y que hacen parte de la información que se requiere en los procesos de apoyo administrativos denominados, la oficina de reserva o back office.

Por una parte, hay que mencionar que la falta de capacitación e interpretación en el manejo de la normatividad aunada a la poca destinación presupuestal para la inversión en tecnología de punta, referente a la estructuración de un buen sistema de seguridad de la información, ha generado que los riesgos por pérdida de la misma, no permita la continuidad del negocio, hecho que de generarse, produce consecuencias graves para la sostenibilidad de la Institución.

De igual manera, el estar ejecutando procedimientos sencillos de copias de respaldo de la información diaria del aplicativo de soporte misional y del contable, de forma semanal y mensual, no garantiza la sostenibilidad de la información. Ésta operación no solamente requiere de estar activa y disponible en tiempo real para ser utilizada desde cualquier terminal que esté conectada al

proceso, ya que requiere del soporte de software de seguridad, hardware y conectividad de última tecnología para poder estar protegida y disponible.

En consecuencia, al Club Militar le falta por implementar el SGSI ya que el acceso, administración y protección a la información presenta una gran debilidad, al no poseer un sistema de administración de seguridad de la información aplicable a toda la infraestructura informática.

Para analizar la situación y proponer mejoras se consultarán las siguientes teorías y sus correspondientes autores que aportan a este tipo de problemática. Iniciamos con Alexander, (2007) quien dice que:òLo único que suelen hacer las empresas, frente a la seguridad de información es actuar de manera reactiva. Al presentarse un incidente, se establece un control .Y pareciera que la labor de las personas encargadas de la seguridad de la información consiste en administrar controles y reaccionar ante la aparición de incidentes de seguridad .Rara vez se actúa de manera proactiva.ò

Por su parte, Montañés, (1996), considera que:ò El programa de seguridad requiere que se lleven a cabo evaluaciones periódicas, para determinar si la siempre cambiante realidad de una organización continúa cubierta en sus aspectos de seguridadò Así mismo Cocho, (2003), opina que:ò La seguridad conseguible con medios técnicos debe completarse con medios organizativos que comprendan una gestión adecuada con responsabilidades internas y ayuda externa de consultoríaò De igual manera, William, (2004), expresa que: ñLa seguridad IP abarca tres áreas fundamentales: autentificación, confidencialidad y gestión de clavesò Por otra parte, Gaspar, (2004), define que: ñPara la elaboración de un plan de contingencia, es decir un conjunto de estrategias y procedimientos preventivos y reactivos que permitan un rápido retorno a una situación suficientemente normalizada como para que la actividad de la organización recupere un nivel aceptable después de una interrupción no prevista de sus

sistemas de información, es de vital importancia planear la implementación de un buen sistema de respaldoò

Para, Picouto, y otros,(2007), advierte que: òTodo sistema Microsoft almacena en su interior información crucial, que puede abarcar varios campos colocados en diferentes lugares y clasificados según su uso; todo esto se guarda siguiendo unas políticas de seguridad basadas en la autentificación de usuarios y contraseñasò Según, la norma ICONTEC, (2004), recomienda seguir la ñISO 27001:2005, Metodología para implementar un Sistema de Seguridad de la Informaciónò Por consiguiente, estos planteamientos se deben tener en cuenta para configurar parámetros de protección, administración, actualización, inversión y disponibilidad del recurso humano, ya que en el Club no se cuenta con un modelo acorde con la metodología de un sistema de seguridad de la información.

Ante la problemática presentada por la carencia de un sistema de seguridad de gestión de la información en el Club Militar, se hace necesario establecer objetivos claros y precisos que conlleven a subsanar dicha situación y permitir un óptimo acceso, administración y protección de la información en aras de asegurar y sostener la continuidad del negocio.

Para tal fin se debe proporcionar al Departamento de Sistemas del Club Militar una serie de metodologías y técnicas que le permitan diseñar e implementar adecuadamente, bajo la óptica del ISO 27001:2005, un sistema de gestión de seguridad de la información en la mencionada organización.

Respecto a la problemática actual, el Club Militar no aplica la norma ISO 27001:2005, que es la guía para implantar un sistema de seguridad de la información, y entre sus requisitos iniciales exige que se debe comenzar por documentar, primero las cláusulas globales que se definen como genéricas y que cubren todo el sistema y están orientadas a dar lineamientos genéricos y las

clausulas focales que son el grupo que da pautas puntuales para instaurar ciertas exigencias.

A continuación, se citan los requisitos que conforman el proceso correspondiente a las clausulas Globales; Enfoque General, Control de Documentos, Control de Registros, Responsabilidad Gerencial, Provisión de Recursos, Capacitación, Conocimiento y Capacidad, Revisión Gerencial, Auditorías Internas, Mejora Continua, Acción Correctiva, Acción Preventiva. Igualmente, al proceso de la cláusulas focales la conforman los siguientes requisitos descritos en la norma ISO 27001:2005, así: Establecer el SGSI, Implementar y Operar el SGSI, Monitorear y Revisar el SGSI, Mantener y Mejorar el SGSI.

Cabe resaltar que cuando se inicia un proyecto de implantación del modelo de seguridad de la información en una empresa, se debe asignar a un responsable del proceso de documentar las cláusulas globales y luego las focales. La documentación es muy importante pues ésta controla por fechas las modificaciones y el estado de las revisiones; cuando aparece el término procedimiento documentado dentro del estándar, significa que el procedimiento debe ser establecido, documentado, implementado y mantenido.

Del mismo modo, el control de la información se basa en un enfoque racional cumpliendo con un plan preestablecido para con el ciclo Planear, Hacer, Verificar y el Actuar, aclarando que el volumen de la documentación depende del tamaño de la organización, el alcance, la complejidad de requerimientos de seguridad y el sistema que se está manejando; la documentación y sus registros pueden estar en cualquier forma o tipo de medio. Esta documentación exige un control y la asignación de un personal responsable, que lleve la supervisión de registros, identificación, almacenaje, protección y disposición con sus registros referentes a toda clase de incidentes.

Por otra parte, no todos los controles son idénticos a cada situación, lo mismo opera para el medio ambiente local y el de restricciones técnicas, como lo expresa, Alexander, ñDiseño y la implementación del SGSI de una organización son influenciados por las necesidades y los objetivos comerciales, los requerimientos de seguridad resultantes, los procesos, los empleados y el tamaño y la estructura de la organizaciónò (2007).

De igual manera, el sistema de seguridad de la información está diseñado para asegurar controles de seguridad adecuados y proporcionados que protejan eficientemente los activos de información, generando confianza entre los clientes y partes interesadas.

El compromiso de la Dirección es de protagonismo en el manejo de un SGSI, pues se debe establecer una política de seguridad de la información, asegurando que se conformen roles y responsabilidades para la seguridad de la misma, así mismo, proporcionar los recursos suficientes para la implementación del SGSI, incluyendo el criterio de aceptación del riesgo y estableciendo un plan de auditorías internas. La auditoría interna al SGSI debe detallar el propósito de la misma pues la norma es muy precisa, esta le asigna a la gerencia del área auditada toda la responsabilidad por las consecuencias de la misma.

Por otra parte, hay que tener en cuenta que la capacitación al personal que está involucrado en la administración, producción y control de los activos de información está sujeta a un análisis y previa evaluación de las necesidades y competencias de acuerdo con su respectivo perfil para asignar las responsabilidades dentro del proceso.

Por consiguiente, la mejora continua del SGSI, es un patrón constante que involucra la política de seguridad de la información, los objetivos de seguridad, los

resultados de la auditoria, el análisis de los eventos monitoreados, las acciones correctivas y preventivas, la capacitación al personal, la revisión gerencial y la auditoria, todo ello enmarcado dentro del proceso de sistema de gestión de calidad.

Como lo señala, Alexander, en su teoría ñDiseño de un sistema de gestión de seguridad de informaciónò, al sugerir que una entidad debe identificar las necesidades y los objetivos comerciales, procesos, requerimientos de seguridad y el tamaño de su infraestructura para posteriormente distinguir entre las normas focales y globales que se han de aplicarò (2007).

Al respecto, asumimos que el Club Militar, no ha hecho esta labor por lo que actualmente presenta confusión al interpretar la norma ISO 27001:2005, generando error en el concepto de proteger los activos de información puntuales y que quizás, éstos no sean los que al momento de ser requeridos para la restauración después de ocurrir un siniestro, permitan la continuidad del negocio.

Por su parte, Montañés, expone que, ñEl programa de seguridad requiere que se lleven a cabo evaluaciones periódicas, para determinar si la siempre cambiante realidad de una organización continúa cubierta en sus aspectos de seguridad. Existen seis pasos o fases a llevar a cabo cuando se evalúa la seguridad de una instalación: Preparación de un plan, identificación y valoración de los activos, identificación de amenazas, análisis de riesgos, ajuste de los controles y preparación del informeò (2006).

Hasta ahora, el Club Militar no posee un diseño de un sistema de gestión de seguridad de la información que le permita, que ante una evaluación, pueda identificar con claridad que los recursos físicos estén adecuadamente salvaguardados.

Por una parte, el cálculo de los riesgos de seguridad de la información incluye normalmente el análisis y la evaluación del riesgo. El análisis del riesgo permite; identificar los activos de la información, verificar los requerimientos legales y comerciales que le son inherentes a los activos, calcular los activos identificados, identificar las amenazas y vulnerabilidades para cada activo y calcular la posibilidad de que estas ocurran.

Una vez cumplido con lo anterior, la entidad debe establecer una clara política de seguridad para apoyar la implementación del SGSI. Se debe utilizar la norma ISO27001:2005, en donde se norma qué elementos obligatorios del proceso de cálculo del riesgo debe contener por ejemplo: Determinación del criterio para la aceptación del riesgo, identificación de los niveles aceptables del riesgo, la cobertura de todos los aspectos del alcance del SGSI y el cálculo del riesgo que debe lograr un claro entendimiento sobre qué factores deben controlarse.

De modo semejante, los activos de información de la empresa, dentro de la importancia del SGSI son fundamentales para una buena implementación del mismo. Es por esto que el análisis y la evaluación del riesgo junto con las decisiones que se tomen giran alrededor de los activos de información identificados.

Como lo señala, Alexander, ñLa ISO 17799:2005 clasifica los activos de información en las categorías siguientes: Activos de información (manuales de usuario, datos, etc.é). Documentos de papel (contratos). Activos de software (aplicación, software de sistemas, etc.é). Activos físicos (Computadores, medios magnéticos, etc.é).Personal (clientes, personal.).Imagen de compañía y

reputación. Servicios (comunicaciones, etc.). Se debe asignar un responsable dueño del activo.ò (2007).

A su vez, para establecer los requerimientos de seguridad en la entidad sin importar su tamaño, éstos se derivan de tres fuentes así: La primera proviene de la evaluación de los riesgos que afectan a la organización. Aquí se determinan las amenazas de los activos, luego se ubican las vulnerabilidades, se evalúa su posibilidad de ocurrencia, y se estiman los potenciales impactos. La segunda, es el aspecto legal. Aquí están los requerimientos contractuales que deben cumplirse. Y la tercera, es el conjunto particular de principios, objetivos y requerimientos para procesar información, que la empresa ha desarrollado para apoyar sus operaciones.

Según, Alexander, ñPara que una amenaza cause daño a algún activo de información, tendría que hacer activar una o más vulnerabilidades del sistema; identificando la amenaza se evalúa la posibilidad de ocurrencia. La vulnerabilidad abarca las debilidades del sistema de seguridad, pero estas no causan daño, simplemente son condiciones que pueden hacer que una amenaza afecte un activoò (2007).

Así mismo, los elementos del análisis del riesgo no pueden verse de manera aislada. Una vez efectuado el cálculo del riesgo por cada activo, en relación con su amenaza, se debe determinar cuáles son aquellas amenazas cuyos riesgos son los más significativos, esto se denomina la evaluación del riesgo.

Por otra parte, se muestran los criterios para determinar los niveles de riesgo: El impacto económico del riesgo, el tiempo de recuperación de la empresa, la posibilidad real de ocurrencia del riesgo y la posibilidad de interrumpir las actividades de la empresa.

Igualmente, los controles pueden reducir el riesgo estimado en dos maneras: a modo de Alexander, significa que, ñReduciendo la posibilidad de que la vulnerabilidad sea explotada por la amenaza y reduciendo el posible impacto si el riesgo ocurriese, detectando eventos no deseados, relacionado y recuperándose de ellosò (2007).

Al respecto, el Club Militar, no realiza el proceso para seguir los lineamientos que traza la norma ISO 27001:2005, la cual exige que a los activos de información se les aplique la metodología para estimar el riesgo e identificar su importancia en la empresa, una vez identificados se debe decidir cuáles son las opciones de tratamiento del riesgo más adecuadas para mitigarlo.

Según lo expresa, Cocho, ñLa seguridad conseguible con medios técnicos debe completarse con medios organizativos que comprendan una gestión adecuada (con responsabilidades internas y ayuda externa de consultoría) y procedimientos que consigan la participación de empleados, proveedores, clientes y accionistasò (2003).

Por consiguiente, el Club debe establecer y mantener un SGSI, Sistema de Gestión de Seguridad de la Información bien documentado, que precise los activos a proteger, el enfoque de la gestión del riesgo, los objetivos y medidas a tomar, así como el grado requerido de aseguramiento.

De acuerdo con lo mencionado anteriormente, para identificar las necesidades de seguridad, la organización parte de tres fuentes principales:

a. La evaluación de los riesgos del Club Militar, identificando las amenazas a los activos, su vulnerabilidad y su impacto potencial.

b. Los requerimientos legales y contractuales del entorno que deben satisfacer a la entidad, sus socios comerciales, los contratistas y los proveedores de servicios.

c. Los principios, objetivos y requerimientos propios para el proceso de la información que el Club ha desarrollado para soportar sus operaciones.

Igualmente, para el desarrollo del marco adecuado del SGSI, la organización debe emprender un proceso de seis pasos que identifiquen y documenten sus objetivos y medidas:

a) Definir una política.

Una vez determinado el alcance del SGSI, el Club Militar debe establecer una clara política de seguridad para apoyar la implementación de la seguridad de la información en el Club. Según, Alexander, ñLa ISO 17799:2005 plantea que el objetivo de la política esé proveer a la gerencia, dirección y apoyo para la seguridad de la informaciónò(2007), además, la dirección del Club debe aprobar la política, y asegurarse de que todos los empleados la han recibido y entienden su efecto en las tareas. Como dice, Alexander ñEn la cláusula 4.2.1 (b) La ISO 27001:2005 plantea los requerimientos con los cuales debe cumplir una política de seguridad.ò(2007).

Actualmente, la entidad no cuenta con un sistema de gestión de seguridad de la información reglado por un acto administrativo, solo sigue algunas recomendaciones emanadas del Plan Estratégico de Tecnología de Información que el Ministerio de la Defensa ha adoptado (PETI), y un plan de contingencia desactualizado que hace referencia a una infraestructura de hardware a nivel de servidores, y de software de aplicaciones comerciales, que se encuentra registrado en el manual del sistema de gestión de la calidad.

b) Definir el alcance del SGSI.

La implementación del SGSI requiere de un plan de contingencia que incluye los elementos referidos a los sistemas de información, equipos, infraestructura, personal, servicios y otros, aplica para la Sede Principal y sus centros vacacionales, direccionado a minimizar eventuales riesgos ante situaciones adversas que atenten con el normal funcionamiento de los servicios de la institución. El procedimiento de selección de los procesos y subprocesos de las operaciones misionales y de apoyo son los más críticos por el volumen de datos que manejan y que operan de frente al cliente en el negocio.

De hecho, en esta organización las operaciones de respaldo o salvamento de la información están dirigidas a las operaciones misionales y de apoyo, pero son excluyentes de las operaciones de ofimática y de control, la cual debe contener una cobertura del 100% de todos los procesos y subprocesos que operan en el negocio. Debe realizarse un inventario de los activos de información ya que actualmente no existe o esta desactualizado.

c) Evaluar los riesgos.

El enfoque y la filosofía para el riesgo en el Club Militar están determinados de manera muy precisa por la ISO27001:2005. En la cláusula 4.2.1(c), se requiere que la organización identifique y adopte un método y un enfoque sistemático para el cálculo del riesgo de sus activos de información. El Club determinará que método de cálculo utilizará.

Por lo tanto, los riesgos que afectan a la seguridad del edificio son entre otros: Inundación, incendios, robos, ataques internos, los cuales pueden ocasionar pérdidas totales o parciales de información, actividades interrumpidas hasta solucionar el problema; de igual forma los cortes prolongados de energía eléctrica, generan caída total de los sistemas y caída de servidores; así mismo los virus informáticos, ocasionan molestias en el sistema, ya que lo degradan y lo hacen más lento, produciendo pérdidas totales o parciales de datos almacenados.

Por otra parte, entre los riesgos que afectan la integridad de los datos están: La pérdida del dominio de sincronización entre los servidores, que ocasiona problemas de comunicación entre la terminal cliente y el servidor; así mismo, los daños en el cableado eléctrico de las estaciones de trabajo, generan incomunicación entre las partes; e igualmente, los problemas con los recursos compartidos de la red, presentan pérdida de información por congestión de solicitudes a equipos o software.

De igual manera, la caída de la base de datos y la falla total o parcial de los sistemas, genera pérdida de información e interrupción en el proceso de continuidad; a su vez la caída de los servidores por fallas mecánicas, ocasiona un colapso total en la operación diaria, hasta su reparación, la cual demanda un tiempo prudencial para su arreglo; y las pérdidas totales o parciales de las

estaciones de trabajo, produce un leve retraso en la operación, pero no por demasiado tiempo, al ser fácil su reposición.

En consecuencia, estas situaciones mencionadas anteriormente, generan pérdidas totales o parciales de hardware y software produciendo interrupción en las actividades de la continuidad del negocio, hasta tanto se pueda solucionar el problema.

d) Gestionar los riesgos.

Entre los elementos obligatorios que el proceso de cálculo del riesgo debe contener y que ICONTEC, lo define en ñLa ISO27001:2005 en su cláusula 4.2.1(c) como determinación del criterio para la aceptación del riesgo, tenemos que documentar las circunstancias bajo las cuales la organización está dispuesta a aceptar los riesgos.ò (2004); por consiguiente, la identificación de los niveles aceptables del riesgo, al margen del tipo de enfoque que se utilice para el cálculo del mismo, deben estar identificados para que la organización los considere aceptables; de igual forma, la cobertura de todos los aspectos del alcance del SGSI y el enfoque escogido por la empresa, para el cálculo del riesgo debe contemplar un análisis exhaustivo de todos los controles presentados en el anexo A de la ISO27001:2005.

Como lo expresa, Alexander, en ñEl cálculo del riesgo debe lograr un claro entendimiento sobre qué factores deben controlarse, en la medida en que estos factores afecten sistemas y procesos que sean críticos para la organización. Las actividades de la gestión del riesgo deben contemplar la relación costo- beneficio y verificar su pragmatismo. Una eficaz gestión del riesgo significa un buen balance entre el gasto en recursos a contar y el deseado grado de protección, y asegurando que los recursos gastados sean correlacionados con la potencial perdida y el valor de los activos protegidos.ò(2007).

e) Seleccionar los objetivos y las medidas de control a implantar.

Continuando, con la seguridad, William, expresa que: ñLa seguridad IP abarca tres áreas fundamentales; autentificación, confidencialidad y gestión de clavesò (2004); el mecanismo de la autentificación opera, desde que se recibe un paquete de información de una fuente que lo ha transmitido, previamente identificada y examinada su dirección I.P., por un software de detección de direcciones. La confidencialidad opera, de modo que verifica que los nodos que se comunican entre sí estén sincronizados y ningún otro sistema los escuche o intercepte. La herramienta de gestión de claves opera el intercambio de las claves que se cruzan entre sí para obtener permisos de transmisión y acceso de la información.

f) Preparar la aplicabilidad.

Como lo señala, Cocho, ñUn sistema se diseña para satisfacer las necesidades de un grupo particular de utilizadores finales. Su entorno es real y puede definirse y observarse detalladamente. Las amenazas contra su seguridad son reales y pueden determinarseò (2003). El Proceso de implementar el Sistema de Gestión de Seguridad de la Información en el Club Militar, tiene como objetivo proteger los activos de información que es lo más valioso que opera de frente a los socios que esperan que la continuidad del negocio no se interrumpa por intromisión de agentes internos o externos que causen daño .Es por esto que se debe preparar la aplicación para que se pueda poner en marcha apegados a la norma de la ISO 27001:2005.

Complementando el tema de seguridad, el autor Picouto, dice: ñUn hacker puede argumentar infinidad de motivos que le lleven a asaltar un sistema de Microsoftò (2007); siendo este el sistema operacional más comercializado en servidores y computadores medianos, es necesario practicar una muy buena

administración de los recursos de seguridad que se encuentran en el mercado local, con el propósito de implementarlos en la plataforma de servidores y computadores que operan en el Club.

Por consiguiente, el Club Militar soporta toda su plataforma de hardware con el sistema operacional Windows de Microsoft, y es imperativo que se realice una política de administración referente a la adquisición e implementación de un programa de seguridad y administración de toda la estructura informática que opera con el sistema operacional de Windows.

Ante la problemática expuesta, se hace urgente y necesario implementar un Sistema de Gestión de Seguridad de la Información, SGSI en el Club, la cual estará enfocada bajo la óptica ISO 27001:2005.

En consecuencia, es necesario mencionar algunos aspectos fundamentales a tener en cuenta: En cualquier tipo de organización para nuestro caso de tipo empresarial, la implantación del modelo que nos ocupa, obedece a un enfoque de modificaciones; el implantar un SGSI, altera el orden del manejo acostumbrado que se viene dando, circunstancia que conlleva a un obvio y esperado efecto de rechazo al cambio o cambios esperados.

Así mismo, es importante señalar, como requisito fundamental la participación y liderazgo de la alta Gerencia, pues su rol es fundamental al momento de la percepción del cambio al interior de la organización, puesto que se debe ver la implantación del modelo como decisión de carácter estratégico. Es por tal motivo que si se quiere realmente realizar una implantación del SGSI, hay que

concientizar los niveles estratégicos y técnicos partiendo de una acertada capacitación.

Por consiguiente, la decisión de la implantación es de carácter democrático; esto es necesario para evaluar diversos puntos de vista, para así, también generar cohesión y crear sinergia entre los diversos niveles que intervienen en la implantación del modelo. Sin embargo, cuando ya se haga efectiva la toma decisoria de la implantación del mismo, debe ser alguien del más alto nivel gerencial al interior de la organización quien asuma la total responsabilidad del proceso, sin permitir sabotajes del mismo, así se definiría como una implantación de régimen único.

A continuación, se muestra un cuadro que contiene las fases y actividades que describen la metodología para implantar el modelo ISO 27001:2005, el cual se compone de once fases, las cuales para cumplir cada etapa deben llevar a cabo una serie de tareas propias denominadas actividades que están interrelacionadas; estas conforman un proceso sistémico que lleva el paso a paso para la realización de la implementación de un sistema de gestión de la seguridad de la información en cualquier entidad, cumpliendo con la normatividad recomendada para llevar a cabo este proyecto.

Cuadro 1.Metodologia para implantar el Sistema de Gestión de Seguridad de Información ISO 27001:2005.

FASES	ACTIVIDADES
a. Entendimiento de los requerimientos del modelo.	Taller con niveles estratégicos y tácticos.
b. Determinación del riesgo.	Etapa Estratégica
	Etapa Táctica
C .Análisis y evaluación del riesgo	Realización de análisis y evaluación del riesgo
	Definición de política de seguridad de información y objetivos
	Evaluación de las opciones para el tratamiento del riesgo
	Selección de controles y objetivos de control
	Elaboración de la declaración de aplicabilidad
d. Elaboración del plan de continuidad del negocio	Realizar el análisis del negocio
	Efectuar análisis del riesgo e identificar escenarios de amenaza
	Elaborar estrategias de continuidad
	Diseñar plan de reanudación de operaciones
	Diseñar procesos de ensayo
e. Implementar y operar el SGSI	Elaborar el plan de tratamiento del riesgo
	Determinar la efectividad de los controles y métricas
f. Monitorear y revisar el SGSI	Detección de incidentes y eventos de seguridad
	Realización de revisiones periódicas al SGSI
g. Mantener y mejorar el SGSI	Implementar las acciones correctivas y preventivas
h .Desarrollo de competencias organizacionales	Entrenamiento en documentación del SGSI
	Entrenamiento en manejo de la acción correctiva y preventiva
	Entrenamiento en manejo de la auditoria interna
i. Redacción del Manual de Seguridad de información	Redacción del Manual de seguridad de información
j. Ejecución de las auditorías internas	Realización de las auditorías internas
k. Obtención de la certificación internacional	Búsqueda de la empresa certificadora
	Realización de la auditoria por parte de la certificadora
	Obtención de la certificación

Fuente: Diseño y Gestión de un Sistema de Seguridad de Información, ISO 27001:2005.

Como ya se ha mencionado, la Alta Gerencia es la responsable del proyecto de implantación y por tanto, se debe asignar un gerente de la organización con la responsabilidad de la gestión del proyecto y sus diversas actividades, de acuerdo con el control que tenga el gerente o encargado de cada fase del ciclo metodológico, a continuación descrito:

a. Fase 1: Taller estratégico con la Gerencia para analizar requerimientos del modelo.

Esta fase es fundamental y usualmente se logra con un taller de dos o cuatro días de duración. Este taller ayuda a que los niveles estratégicos y tácticos decidan democráticamente la implantación del modelo en el Club Militar, previamente autorizados por el Consejo Directivo.

b. Fase 2: Determinación del alcance del modelo.

La ISO 27001:2005 está concebida bajo la óptica de sistemas de informática. El alcance dependerá de muchos factores. Uno de ellos será los recursos disponibles, la experiencia en la implantación y la complejidad de algunos procesos en relación con el riesgo de la información.

Siendo la primera vez que se pretende implantar el modelo, éste no debe ser tan ambicioso y seleccionar procesos complejos que pudieran hacer fracasar la implantación del SGSI, así como actualmente opera el sistema de administración por módulos en el Club sería un buen proyecto a realizar.

Como he dicho arriba, la determinación del alcance obedece a dos etapas que se deben implementar en el Club Militar. La primera es la estratégica y la otra la táctica, que es la netamente técnica. La etapa estratégica determinará el alcance del modelo, está dirigida a resolver la pregunta ¿cuál o cuáles procesos son los principales para implantar el modelo? Es por tal motivo que en la presente etapa se deben identificar los factores críticos de éxito y por otro lado, identificar los procesos puntuales de la organización. Es importante resaltar que los factores críticos del éxito son aquellas características organizacionales de quien depende

el éxito o el fracaso de la entidad. Así mismo, el método para identificar tanto los procesos como los factores críticos, es la confección de una matriz, cuyo objetivo es identificar aquellos aspectos que mayor impacto tienen en los factores críticos del éxito; estos procesos con mayor impacto son los principales a tener en cuenta para la implantación del modelo.

Respecto a, la etapa táctica, esta consiste en aplicarle a los procesos identificados en la etapa estratégica, como resultado de la estructuración de la matriz descrita anteriormente, la metodología de las elipses; entendida ésta como la identificación detallada de los componentes de cada proceso al interior y al exterior de la organización.

Conviene tener en cuenta, que la ejecución de las etapas estratégicas y tácticas para determinar el alcance, debe ser realizada por equipos de trabajo interdisciplinarios, conformados por integrantes de los procesos organizacionales que se están analizando. Esto es vital, porque solo los responsables del proceso son los que más conocimientos tienen sobre la problemática y la naturaleza del mismo.

c. Fase 3: Efectuar un análisis y evaluación del riesgo.

La metodología a utilizar en esta fase y sus actividades deberá atender a los siguientes aspectos. En primer lugar, identificar detalladamente todos los Activos de información, comprendidos en el modelo del alcance de la organización. Seguidamente, para conocer el impacto de cada activo de información en la entidad, se debe tasar cada activo con base en su confidencialidad, integridad y disponibilidad. Una vez se efectúa la tasación, el

Club, decidirá cuáles son aquellos activos de información considerados más importantes.

A continuación, el siguiente paso, es iniciar el análisis del riesgo para definir con un estimado del mismo, cuánto se aplica a cada activo de información. Del ejercicio anterior se escogen los activos de información que como resultado del análisis del riesgo se les considera más puntuales, críticos o importantes y a éstos se les efectuará una evaluación de riesgo.

Así mismo, el resultado de la evaluación del riesgo, le permite al Club Militar determinar aquellos activos de información más significativos; es a partir de este momento que empieza la etapa de evaluar las opciones para el tratamiento del riesgo. Entonces, el Club entrará a decidir en relación con el riesgo de los activos, a cuáles se les reducirá, evitará, aceptará y transferirá el riesgo. Estas decisiones de carácter estratégico son las que deberá tomar la entidad, teniendo en cuenta los costos involucrados, la imagen y la cultura organizacional de la entidad.

d. Fase 4**:** Elaboración del Plan de continuidad del negocio.

A partir de esta fase, se entenderá como ya implantado el SGSI, es por tal motivo que de ahora en adelante las subsiguientes fases a exponer, se enfocan al mantenimiento y verificación de los procesos que hacen sustentable y comprobable la existencia de la implementación del SGSI en la empresa.

Como ya se ha mencionado y explicado en las anteriores fases, al igual que su metodología de la implementación del SGSI con el ciclo metodológico de la implantación del modelo según la ISO 27001-2005, esta fase es el inicio de una nueva etapa dentro de todo el proceso de afianzamiento posterior a la implantación del modelo; por tal motivo, arranca en la fase cuatro de acuerdo a lo estipulado por la norma rectora del modelo a implantar; la ISO 27001:2005.

Como lo expone, Martínez, ñPara la elaboración de un plan de contingencia, es decir un conjunto de estrategias y procedimientos preventivos y reactivos que permitan un rápido retorno a una situación suficientemente normalizada, no se debe minimizar los tiempos y costosò,(2004). Por lo anterior, se requiere que el Club Militar no lo mire como un proyecto que tenga duración a corto plazo y menos, medirle su rentabilidad, ya que la seguridad forma parte de los objetivos estratégicos de la entidad y es responsabilidad de la alta dirección que continúen las operaciones y funciones, después de que ocurra cualquier incidente que la interrumpa, permitiendo la continuidad del negocio.

e. Fase 5: Implementación y operación del SGSI.

Esta fase tiene a su vez, dos actividades para llevarla a cabo: Primero, hay que elaborar el plan de tratamiento del riesgo, utilizando como insumos la decisión de las opciones para el tratamiento del riesgo y la selección de los controles tal como se hizo en la fase tres, es entonces que se debe generar un plan pormenorizado de las responsabilidades, los recursos, tiempos y mecanismos de control para implantar las estrategias escogidas de tratamiento de riesgo.

En segunda medida, hay que determinar la efectividad de los controles y la métrica o los indicadores de gestión; aquí se debe determinar qué indicadores de

gestión se utilizarán para identificar la efectividad de los controles seleccionados y también definir cómo se va a utilizar estas mediciones para evaluar y producir resultados comparables; en resumen, lo que se busca es que el Club defina sus indicadores para determinar con evidencias objetivas si los controles elegidos arrojan resultados.

f. Fase 6: Monitoreo y revisión del SGSI.

Una vez implementado el modelo y éste se encuentre funcionando en el Club Militar, es necesario haber diseñado los mecanismos para monitorear y revisar su desempeño y poder cerciorase de que el SGSI opera como estaba planeado. Las tareas para el desarrollo de la presente fase son dos: En primer lugar, la detección de incidentes y eventos de seguridad. La entidad debe tener los procedimientos respectivos para poder rápidamente reportar los incidentes y detectar los eventos, tomar acciones y evitar que se conviertan en alteraciones de seguridad. Lo siguiente, es la realización de revisiones periódicas al SGSI. Se deben desarrollar los procedimientos que, aseguren que de manera periódica, se revisa el funcionamiento del SGSI y se verifica la efectividad de los controles instaurados.

g. Fase 7: Mantenimiento y mejoramiento del SGSI.

En esta fase se debe lograr establecer un mecanismo que permita operar la evidencia objetiva de que el SGSI se mantiene y se mejora constantemente. Es importante ejercer la costumbre de estar revisando periódicamente estadísticas, observar tendencias, y con base en esa información, se elaboran e implementan las acciones correctivas y preventivas. Al respecto, se debe tener documentado los procedimientos (exigencia de la norma) y haber generado en la cultura de la

organización el hábito de desarrollar acciones correctivas ante el incumplimiento de requerimientos.

h. Fase 8: Desarrollo de competencias organizacionales.

La implementación del SGSI, ISO27001:2005, exige que la institución tenga ciertas competencias organizacionales, desarrolladas en el personal que labora para el mismo. Se requieren tres competencias básicas, las cuáles a su vez componen tres tareas de desarrollo de la presente fase:

En primer lugar, se debe establecer un entrenamiento en la documentación del SGSI; es decir el personal debe tener destrezas para poder documentar procedimientos, políticas, instrucciones de trabajo y saber identificar registros del Sistema de seguridad de Información. Lo siguiente, será realizar entrenamiento en el manejo de la acción correctiva y preventiva. El Club debe recolectar datos de todas las ocurrencias de incidentes de seguridad significativos del SGSI y con base en las evidencias objetivas de ocurrencias, se vean las tendencias y de tal manera se desarrollen acciones preventivas para evitar que la no conformidad se presente. Finalmente, hay que establecer un entrenamiento en el manejo de auditoría interna, tal como lo exige la cláusula seis de la norma, se requiere que la entidad se audite a sí mismo para demostrar que su sistema se mantiene y que busca nuevas oportunidades de mejora.

i. Fase 9**:** Redacción del manual de seguridad.

La actividad básica de esta fase es la redacción del Manual de Seguridad y es básicamente un documento, con el paso a paso de los procedimientos y métodos de aplicación y ejecución de los procesos de mantenimiento del SGSI posterior a su implementación. Actualmente, en la organización no existe un manual, solo unas guías que aplican al proceso de copias de seguridad, y están desactualizadas ya que en momentos de realizar operaciones de recuperación, éstas no han sido apropiadas por la confusión que presentan, al no estar definidas claramente las instrucciones por cada procedimiento que se ejecuta.

J. Fase 10: Ejecución de las auditorías internas.

Como ya se expresó en la fase ocho literal c, es necesario la auditoría al proceso de funcionamiento del SGSI; Sin embargo, en la presente fase lo que se debe determinar es el medio, mediante el cual se va a realizar la auditoría; si se va a hacer internamente o se va a contratar un auditor externo. Por consiguiente, es importante definir, que, si el tipo de auditoría que se va a aplicar al Club es interna, se hará necesario capacitar al personal que va a ejercer esta labor a través de un ente certificador, con el propósito de mejorar las competencias de los participantes y obtener un resultado preciso y acorde con el sistema que se va a auditar. Pero, si es con auditoría externa, el ente certificador debe estar certificado por una entidad de reconocimiento internacional.

k. Fase 11: Obtención de la certificación internacional.

La certificación internacional, debe ser la culminación de todo el esfuerzo realizado en la implementación del sistema de gestión de seguridad de la información en el Club Militar. Por tal motivo, la certificación consiste en obtener un aval muy importante para mostrar a terceros que se tiene un Sistema de

Gestión de Seguridad de Información implantado de conformidad con el estándar ISO 27001:2005 y que una empresa acreditada para dicho efecto, da fe al respecto; esto se lleva a cabo en tres actividades: Búsqueda de la empresa certificada, realización de la auditoría de la empresa acreditadora y obtención de la acreditación.

En síntesis, la implantación de un modelo ISO 27001:2005, tiene que contemplarse como un proyecto, el cual tiene tiempos asignados a actividades, consumo de recursos, e incluir un Gerente de Proyecto que lo controla y una alta Gerencia que la apoya; así mismo, el tiempo para implementar el SGSI en la entidad, dependerá de varios factores como: El alcance del modelo, los recursos disponibles, la capacitación del personal, la participación de la gerencia y la prioridad que se le dé al proyecto.

Para concluir, se recomienda que el Club Militar, debe iniciar un proceso de planeación estratégica, en donde proyecte a un corto y mediano tiempo el proyecto de implementación del Sistema de Gestión de Seguridad de la Información, basado en la normatividad de la ISO 27001:2005, la cual, como ya se ha descrito en forma general, contiene la metodología que se requiere para la implementación del SGSI, recurriendo a la asesoría externa, el apoyo financiero y la gestión del talento humano que se requiere para realizar este proceso, pues los socios esperan que la continuidad del negocio no se vea interrumpida por la carencia de implementar un SGSI.

REFERENCIAS.

Alexander, A. G. (2007). *Diseño y gestión de un sistema de seguridad de informacion.* Bogotá - Colombia: Alfaomega colombiana s.a.

Cocho, J. M. (2003). *Riesgo y Seguridad de los Sistemas Informáticos.* Valencia España: Editorial de la UPV.

Éstandares, F. d. (2004). *William Stallings.* Madrid: Pearson Educación S.A.

ICONTEC 27001, U.I. (2004). ISO 27001:2005. Bogotá.

Internet, H. y. (2007). *Fernando Picouto Ramos, Iñaki Lorente Perez,Jean Paul Garcia,Moran, Antonio Angel Ramos.* Madrid: Alfaomega grupo editor, S.A de C.V.

Martínez, J. G. (2004). *Planes de Contingencia.* Madrid: Ediciones Díaz de Santos, S.A.

Montañés, R. B. (1996). *Auditoria de los sistemas de información.* Valencia, España: Servicio de publicaciones camio de Vera.