ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

TEMA:

“DISEÑO DE AUDITORÍA DE UN SGSI – SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, BASADO EN ISO 27001**”**

EXAMEN DE GRADO (COMPLEXIVO)

PREVIO A LA OBTENCIÓN DEL GRADO DE:

MAGÍSTER EN SEGURIDAD INFORMÁTICA APLICADA

MIGUEL ANGEL CHANG AGUILAR

Guayaquil – Ecuador

AÑO

2016

AGRADECIMIENTO

A mi esposa Teresita por su amor, su invaluable apoyo y soporte.

DEDICATORIA

A mi familia, por ellos mis esfuerzos y ganas de superarme.

TRIBUNAL DE SUSTENTACIÓN

Ing. Lenin Freire C.
DIRECTOR DE LA MSIA

Ing. Juan Carlos García
PROFESOR DELEGADO POR
LA UNIDAD ACADÉMICA

RESUMEN

El presente trabajo pretende proporcionar una guía para llevar a cabo una auditoria a un SGSI – Sistema de Gestión de Seguridad de la Información, implementado de manera formal o no, durante el desarrollo de la guía se podrán identificar las actividades clave para llevar a cabo esta actividad y realizar una verificación independiente del grado de implementación del SGSI, de los controles detallados y de la madurez de los procesos del SGSI basado en la norma NTE INEN-ISO/IEC 27001:2011 [1].

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

CAAT	Técnicas de Auditoría asistidas por Computadora
CEO	Chief Executive Officer
CIO	Chief Information Officer
CMMI	Capacity and Maturity Model Integration
IEC	International Electrotechnical Commission
INEN	Instituto Ecuatoriano de Normalización
ISO	International Organization for Standardization
NTE	Norma Técnica Ecuatoriana
PDCA	Plan, Do, Check, Act
PHVA	Planificar, hacer, verificar y actuar
SGSI	Sistema de Gestión de la Seguridad de la Información

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La seguridad de la información y los SGSI ya nos van acompañando durante un lapso de tiempo importante, hay muchos productos disponibles, abundante oferta académica, certificaciones y empresas certificadas, proyectos en ejecución, profesionales estudiando la norma y universidades incluyéndola en sus programas de estudio.

El auge no es deliberado, la tendencia mundial hacia la automatización trae varias décadas de cola, el internet y la nube le han dado una perspectiva más amplia al uso y tránsito, almacenamiento y consumo de la información del negocio, que sin lugar a dudas preocupa y es factor clave a considerar.

Todo proceso bien dirigido debe además ser sometido a una validación, con más credibilidad por supuesto si es hecha por un ente externo, y es en ese sentido que el presente trabajo pretende proporcionar una guía para llevar a cabo esa evaluación y mostrar resultados que permitan a la alta gerencia conocer y administrar este importante aspecto en la empresa.

CAPÍTULO 1

GENERALIDADES

1.1. Descripción del problema

Muchas empresas están conscientes de la necesidad de tomar medidas en cuanto a la seguridad de su información, en mayor grado unas y en menor grado otras. Esta necesidad lleva a las empresas con mayor atención en este tópico a emprender actividades para alinearse hacia la construcción de un SGSI – Sistema de Gestión de Seguridad de la Información, y mejorar el nivel de control en sus procesos, principalmente en los procesos que tienen alta demanda de tecnología, además a asegurar la información que: transita en sus redes, se encuentra contenida en sus documentos, es procesada en sus sistemas y almacenada en

hojas de cálculo, almacenada en sus servidores o en la nube, en contenida en la cabeza de las personas, y demás contenedores identificados o no.

Ante tan diverso escenario y diversidad de iniciativas, es una labor complicada para el CIO[1] y para el CEO[2] llegar a un nivel aceptable de seguridad que satisfaga el "apetito de riesgo" si aquello se encuentra definido o que nos ponga al menos en una situación de saber ¿Dónde estamos? en cuanto a este importante y no tan novedoso, pero desatendido mayormente aspecto en la organización.

"No hay viento favorable para quién no sabe a dónde va" Séneca. Frase que plantea una situación real para la alta dirección preocupada de la seguridad de la información y que quizá escucha unilateralmente los planes y avances, proyectos e iniciativas del área responsable de la seguridad de la información en la empresa, pero sin saber si el avance es suficiente, relevante, efectivo, eficiente, o da los resultados deseados.

Y es que gran proporción de iniciativas de seguridad son reactivas, entendiéndose como reactivas a acciones emprendidas posterior a ocurrido un incidente de seguridad de la información, por lo tanto el planteamiento de hacer algo debe alinearse a que la organización no debe encontrarse en una situación de

[1] CIO - Chief Information Officer
[2] CEO - Chief Executive Officer

incumplimiento o afectación para recién entrar en materia y peor aún comenzar a tomar iniciativas sin una orientación clara, o que aparentemente carezca de efectividad, orientación, alineamiento u objeto.

1.2. Solución propuesta

Ante la falta de visibilidad en procesos críticos, es necesario realizar una revisión independiente (auditoría) para proporcionar a la dirección esa claridad, certeza en cuando al funcionamiento y eficacia de las iniciativas de seguridad hacia un SGSI.

El desarrollo de una auditoría del SGSI se base en un proceso normal de auditoría donde se establecen actividades de Planificación, Ejecución y Finalización; esta última incluye informe y seguimiento de la auditoría. El presente trabajo permitirá guiar esos pasos y poder planificar, ejecutar y finalizar una auditoría a un SGSI basado en ISO 27001.

Es por lo tanto que la ejecución de la guía de trabajo sea realizada por un ente con independencia organizacional y profesional al área auditada para asegurar la mayor objetividad.

El esquema de trabajo para la revisión se establece:

- PLAN: Definición del plan de trabajo y alcance de la revisión del SGSI.

- PLAN: Identificar información necesaria y elaborar el requerimiento inicial de información y plan de entrevistas.
- EJECUCIÓN: Verificar la información disponible y hacer corroboración con entrevistas y observación en sitio.
- EJECUCIÓN: Revisar cumplimiento de controles y madures de procesos de seguridad de información y del SGSI.
- EJECUCIÓN: Verificar la evaluación de riesgos de la organización y las medidas preventivas-correctivas tomadas como parte de ese proceso.
- FINALIZACIÓN: Elaborar borrador de informe. Oportunidades de mejora resumidas y detalladas.
- FINALIZACIÓN: Revisión de borrador de informe, madurez de los procesos, grado de cumplimiento e inclusión de observaciones del auditado.
- FINALIZACIÓN: Entrega de informe final.
- SEGUIMIENTO: Verificar el plan de trabajo de implementación de oportunidades de mejora aplicables y documentación de mejora continua del SGSI.

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA AUDITORÍA DEL SGSI

2.1 Planificación de la auditoría del SGSI

La planificación de la auditoría del SGSI es la fase donde se establece el trabajo a realizar, los tiempos de ejecución, la conformación y definición de las responsabilidades del equipo auditor, localidades de la empresa que requieren ser visitadas, entre las principales tareas.

El enfoque en esta importante etapa se basa en primera instancia en comprender la definición y el alcance de implementación del SGSI en la organización y en segundo

lugar identificar en detalle los controles implementados por la organización como parte de las iniciativas de seguridad de la información.

La organización podría haber adoptado varios de los enfoques o iniciativas de seguridad de información disponibles, por lo cual es importante en esta instancia obtener ese detalle y comprender el enfoque metodológico que se ha utilizado para poder guiar la revisión y desde el punto de vista del auditor poder identificar las consideraciones de la implementación.

La auditoría puede ser realizada por personal interno de la organización, capacitado para el efecto, o por personal externo especializado, en cualquiera de los casos es necesario considerar los ya mencionados aspectos de independencia profesional y organizacional necesarios para llevar a cabo esta labor.

En cuanto al trabajo a realizar o alcance, este se debe enfocar en dos aspectos importantes:

- El sistema de gestión de seguridad de la información.
- Los controles detallados que la organización ha decidido implementar, detallados en la Declaración de aplicabilidad.

En cuanto a los tiempos de ejecución, estos van a depender del alcance y del tamaño del equipo auditor.

En cuanto a la conformación y responsabilidades del equipo auditor se sugiere:

- Capacidad profesional o competencia para la asignación.

- Conocimiento de sistemas de gestión de seguridad de la información, al menos se requiere nivel de auditor interno ISO 27001.
- Conocimiento o experiencia en implementación/auditorías de sistemas de gestión de seguridad de la información o controles detallados.

Para lograr una mejor planificación existen varias recomendaciones, se requiere:

- "Lograr una comprensión de la misión, los objetivos, el propósito y los procesos de negocio, incluyendo los requerimientos de información y procesamiento, tales como disponibilidad, integridad, seguridad y tecnología del negocio y de confidencialidad de la información.
- Revisar papeles de trabajo anteriores, si aplica.
- Entender los cambios en el negocio del auditado.
- Identificar los contenidos específicos tales como políticas, estándares y directrices requeridos, procedimientos y estructura de la organización.
- Realizar un análisis de riesgos para ayudar a diseñar el plan de auditoría." [2], entre los principales puntos a considerar.

La primera parte de la planificación de la auditoría debe considerar realizar una reunión de inicio de auditoría o también se la puede referir como "kick off"[3] del proyecto si la auditoría es realizada por un externo.

[3] Kick off – Reunión inicial de un proyecto.

En esta reunión se presentan los objetivos de auditoría y el plan de trabajo inicial, similar al presentado en la figura 1.

Nombre de tarea	Duración	Comienzo	Fin
- Inicio del proyecto	5 días	lun 03/01/11	vie 07/01/11
Entregar solicitud inicial de información	1 día	lun 03/01/11	lun 03/01/11
Definir plan de trabajo y cronograma detallado	3 días	lun 03/01/11	mié 05/01/11
Realizar la sesión de inicio (Kick Off)	1 día	jue 06/01/11	jue 06/01/11
Presentar Plan de Gerenciamiento del Proyecto	1 día	vie 07/01/11	vie 07/01/11
Presentar el Cronograma de Actividades del Proyecto	1 día	vie 07/01/11	vie 07/01/11
- Levantamiento de información	20 días	lun 03/01/11	vie 28/01/11
Revisar documentación relacionada con la gestión de seguridad de la información	10 días	lun 03/01/11	vie 14/01/11
Ciclo de entrevistas	15 días	lun 10/01/11	vie 28/01/11
Estudio de la documentación	10 días	lun 17/01/11	vie 28/01/11
- Revisar cumplimiento	20 días	lun 17/01/11	vie 11/02/11
Revisar las sustentaciones presentadas	20 días	lun 17/01/11	vie 11/02/11
Incorporar los comentarios y sugerencias	10 días	lun 31/01/11	vie 11/02/11
Verificara la ejecución de pruebas de seguridad, los resultados obtenidos, y la ejecución de planes de acción	5 días	lun 31/01/11	vie 04/02/11
- Evaluar riesgos y controles generales de TI	17 días	lun 07/02/11	mar 01/03/11
Entender la arquitectura y características de los activos de TI	5 días	lun 07/02/11	vie 11/02/11
Definir criterios de evaluación de riesgos	4 días	mar 08/02/11	vie 11/02/11
Entrevistas con funcionarios seleccionados	7 días	jue 10/02/11	vie 18/02/11
Analisis de riesgos de activos de TI	5 días	lun 21/02/11	vie 25/02/11
Documentar resultados y plan de acción/remediación	5 días	mié 23/02/11	mar 01/03/11
- Cierre del proyecto	2 días	mié 02/03/11	jue 03/03/11
Preparar y presentar entregables del proyecto	1 día	mié 02/03/11	mié 02/03/11
Realizar presentación ejecutiva de resultados	1 día	jue 03/03/11	jue 03/03/11

Figura 2.1 Cronograma de la auditoría

Cubierta la primera parte, avanzamos en la segunda parte de la planificación que consiste en identificar la información necesaria o requerimiento de información inicial y establecer un plan inicial de entrevistas con los principales roles que en la organización interactúan en torno a un SGSI.

La información relevante de acuerdo al alcance de la auditoría se debe considerar en el requerimiento de información es:

- Auditoría al SGSI. Se deben considerar los documentos obligatorios según la norma NTE INEN ISO/IEC 27001:2011 que son:
    - Declaraciones documentales de la política y de los objetivos del SGSI;
    - El alcance del SGSI;

  - Los procedimientos y mecanismos de control que soportan el SGSI;
  - Una descripción de la metodología de gestión de riesgos;
  - El informe de evaluación de riesgos;
  - El plan de tratamiento de riesgos;
  - Los procedimientos documentados que necesita la organización para asegurar la correcta planificación, operación y control de sus procesos de seguridad de la información, y para describir cómo medir la eficacia de los controles;
  - Los registros requeridos por esta norma;
  - La Declaración de aplicabilidad.
- Para la revisión de los objetivos de control y controles específicos, es necesario solicitar:
  - La identificación de los activos de información sobre los cuales se va a gestionar la seguridad de la información, o en su defecto la documentación de ejecución de una evaluación de riesgo, la más reciente, para verificar que los controles implementados corresponden a una decisión técnica de implementación en base al tratamiento de riesgos y de acuerdo al enfoque adoptado por la organización.

Las entrevistas deben orientarse a validar los procesos descritos en la documentación solicitada, y de cierta forma podremos ir cruzando información para poder concluir posteriormente sobre el SGSI, la entrevista se orienta de forma directa

a las competencias y procesos de los cuales el entrevistado es responsable. Las entrevistas además se deben realizar en varios niveles para efectos corroborativos:

- Entrevistas de nivel ejecutivo
- Entrevistas de nivel administrativo
- Entrevistas de nivel operacional

2.2 Ejecución de la auditoría del SGSI

Una vez cubierta la planificación, y aprobada, se inicia con el trabajo detallado de la auditoría, la ejecución de la auditoría se orienta específicamente por ejecutar lo planeado y evitar cualquier desviación.

A este punto el equipo auditor cuenta con:

- Documentación de la empresa relacionada con el SGSI;
- Entrevistas coordinadas con personal clave de la organización en funciones de dirección, planificación, operación y control del SGSI o de los controles específicos.

Dentro de la ejecución, y para asegurar el correcto enfoque a riesgos, es necesario que el auditor valide lo siguiente:

- Que los activos de información [4] se encuentran identificados, llegando a validar inclusive los criterios sobre los cuales se basó la identificación y documentación de todo el proceso de identificación.
- Que la metodología de gestión de riesgos sea enmarcado en las necesidades y contexto del negocio.
- Que los criterios para la identificación, análisis y valoración de riesgos se hayan aplicado sobre todos los activos y se haya documentado todo el proceso.
- El cumplimiento de los procesos del SGSI y que los registros se llevan a cabo en la organización.
- Exista una Declaración de aplicabilidad y que está ha sido entendida y aprobada por la dirección.
- Cualquier otra documentación que presente evidencia sobre la existencia del SGSI, y el compromiso de la dirección en su definición, apoyo e implementación, así como la provisión de los recursos necesarios.

La revisión de la documentación además implica conocer en detalle las definiciones que la organización tiene por escrito, conocer el método de la organización para formalizar sus procesos y evaluar si todas las definiciones se encuentran formalizadas o van en ese camino:

[4] Activos de información – cualquier bien que tiene valor para la organización.

- El auditor deberá revisar y entender la estructura organizacional, e identificar si la seguridad de la información tiene ámbito a un alto nivel en la organización o se limita a la existencia de roles operativos en el negocio.
- Se deberán validar políticas existentes y que no sean parte de la documentación formal obtenida.
- Se deberá validar el diseño de los procesos y controles de seguridad de la información que la organización ha reconocido y formalizado hasta el momento.

Todo lo revisado y establecido como parte de la documentación debe irse verificando en las entrevistas con el personal, realizando validaciones simples y no documentadas para corroborar que lo diseñado y definido es lo que efectivamente se está haciendo. El nivel de validación se puede realizar principalmente en las entrevistas con el personal operativo en la organización.

A este punto, el auditor podrá ir identificando oportunidades de mejora, que de hecho en algunos casos podrían ser implementadas por la organización. En un enfoque de entrega de valor por parte de la auditoría, estas mejoras rápidas (cortas) o quick wins (como se les dice en inglés) pueden ser informadas e implementadas sin esperar hasta el final del trabajo, haciendo que la organización vea resultados desde etapas tempranas.

Es necesario además que el auditor que ya cuenta con un conocimiento más preciso de la organización, de sus procesos y de las personas que ejecutan esos procesos;

avance en la revisión y realice análisis más detallados que podrían incluir ejecución de pruebas técnicas o revisiones administrativas sobre lo definido y sobre el funcionamiento operativo de estas definiciones.

Revisar el cumplimiento de controles va más allá de verificar si el control en diseño (o también referido “en papel”) es correcto y considera todos los aspectos para reducir el riesgo a niveles aceptables.

Los procedimientos de auditoría [3] para verificar, probar y evaluar pueden incluir:

- El uso de CAATs.
- Uso de software especializado.
- Técnicas de elaboración de diagramas de flujo.
- Uso de registros de los sistemas.
- Revisión de la documentación.
- Observación y consultas.
- Inspección y verificación.
- Revisión del rendimiento de controles.

En cualquiera de los casos, el auditor debe recopilar la evidencia de la prueba y concluir sobre la operación o implementación del control.

Durante la ejecución se puede realizar una evaluación de madures de los procesos del SGSI, la mejor guía para aplicar esta comparación de madurez es la guía del CMMI.

Esta evaluación no es obligatoria pero permite tener completa claridad de la madurez de los procesos del SGSI en comparación con su estado actual y para la empresa sería un valor agregado importante.

Las escalas genéricas de madurez [4], planteadas por el CMMI[5], para evaluar procesos se detallan en el siguiente cuadro:

Modelo Genérico de Madurez
0 No Existente- Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.
1 Inicial- Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques *ad hoc* que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.
2 Repetible- Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.
3 Definido- Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.
4 Administrado- Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.
5 Optimizado- Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

Figura 2.2 Escalas de Madurez del Proceso

Para procesos de seguridad se cuenta ISO [5] ha desarrollado una guía más detallada:

[5] CMMI – Capacity and Maturity Model Integration del CEI.

Tabla 1 Escalas de Madurez de Procesos de Seguridad de la Información

NIVEL DE MADUREZ DE CONTROLES ISO/IEC 27001:2005				
Nivel	**Tipo de Nivel**	**Descripción**	**Característica**	**Implicaciones**
0	**No existente** (No existe) (0%)	No ha reconocido la aplicación de este control. Las responsabilidades de seguridad no están asignadas. Esta situación puede ser formalizada, generando un "No Aplica".	En éste nivel hay una ausencia completa de cualquier proceso de control reconocible o procedimientos relacionados. La organización aún no ha reconocido a la seguridad de la información como un punto a tratar.	La organización no tiene la capacidad para estar en cumplimiento aún con el mínimo nivel.
1	**Inicial** (Diseñado) (20%)	Reconoce la necesidad de este control, pero recién se están iniciando acciones para su implementación. La administración de seguridad es reactiva y no medible.	Hay alguna evidencia que la organización reconoce que los controles y los procedimientos relacionados son importantes y necesitan ser tratados. Sin embargo no existen ni están documentados. No existe un proceso de divulgación, los empleados no están conscientes de su responsabilidad por las actividades del control. La efectividad operativa de las actividades del control no se evalúa sobre una base regular. Las deficiencias del control no son identificadas.	No existen suficientes controles y documentación para apoyar la afirmación de la gerencia. El nivel de esfuerzo para documentar, probar y remediar los controles es muy significativo.
2	**Repetible pero intuitivo** (Implementado Parcial) (40%)	Ha implementado este control y las responsabilidades de seguridad están asignadas al Responsable correspondiente. Existe un nivel de documentación básica y se pueden generar rastros de auditoría pero no son analizados.	Los controles, las políticas y procedimientos relacionados existen, pero no siempre completamente documentados. Existe un proceso de divulgación pero no está documentado. Los empleados podrían no estar conscientes de sus responsabilidades por las actividades del control. La efectividad operativa de las actividades del control no se evalúa adecuadamente sobre una base regular y el proceso no está documentado.	Aunque existen controles, políticas y procedimientos, no hay suficiente documentación para apoyar la certificación y la afirmación de la gerencia. El nivel de esfuerzo para documentar, probar y remediar los

NIVEL DE MADUREZ DE CONTROLES ISO/IEC 27001:2005				
Nivel	**Tipo de Nivel**	**Descripción**	**Característica**	**Implicaciones**
			Las deficiencias del control pueden ser identificadas, pero no son resueltas de manera oportuna.	controles es significativo.
3	**Proceso definido** (Implementado Total) (60%)	Tiene el control implementado alineado con programas de concientización en seguridad para los usuarios, políticas existentes y procedimientos de seguridad. Está enmarcado en un plan de seguridad manejado a través de análisis de riesgos repetitivo.	Los controles, las políticas y procedimientos relacionados, existen y están adecuadamente documentados. Existe un proceso de divulgación adecuadamente documentado. Los empleados están conscientes de sus responsabilidades por las actividades del control. La efectividad operativa de las actividades del control se evalúa sobre una base periódica (por ejemplo, cuatrimestralmente); sin embargo el proceso no está completamente documentado. Las deficiencias del control son identificadas y resueltas de manera oportuna.	Existe suficiente documentación para apoyar la certificación y afirmación de la gerencia. El nivel de esfuerzo para documentar, probar y remediar los controles puede ser significativo dependiendo de las circunstancias en la organización.
4	**Gestionado y medible** (Probado) (80%)	Revisa indicadores de comportamiento del control. Se realizan periódicamente análisis con el fin de mejorar la eficiencia del control.	Los controles, las políticas y procedimientos relacionados, existen y están adecuadamente documentados, y los empleados están conscientes de su responsabilidad por las actividades de control. Existe un proceso de divulgación adecuadamente documentado y monitoreado, pero no siempre reevaluado para reflejar procesos mayores o cambios organizacionales. La efectividad operativa de las actividades del control se evalúa sobre una base periódica (por ejemplo, semanalmente); y el proceso está adecuadamente documentado. Hay un limitado, primariamente táctico, uso de la	Existe suficiente documentación para apoyar la certificación y afirmación de la gerencia. El nivel de esfuerzo para documentar, probar y remediar los controles puede ser poco significativo dependiendo de las circunstancias en la organización.

NIVEL DE MADUREZ DE CONTROLES ISO/IEC 27001:2005				
Nivel	**Tipo de Nivel**	**Descripción**	**Característica**	**Implicaciones**
			tecnología para documentar procesos, objetivos de control y actividades.	
5	**Optimizado** (Probado y Mejorado) (100%)	Realiza análisis periódicos de costo/beneficio para futuros cambios o mejoras del control. Puede impactar en objetivos estratégicos a nivel de TI o negocio.	El nivel 5 cumple todas las características del nivel 4. Existe un programa de control y gestión de riesgo, de manera que los controles y procedimientos están bien documentados y son reevaluados continuamente para reflejar procesos mayores o cambios organizacionales. Se usa un proceso de auto medición para evaluar el diseño y efectividad de los controles. La tecnología se lleva a su máxima extensión para documentar procesos, objetivos de control y actividades, identificar brechas, y evaluar la efectividad de los controles.	Se mantienen las implicaciones del nivel 4. Es posible una mejor toma de decisiones gracias a información de alta calidad y oportuna. Los recursos internos son usados efectiva y eficientemente. La información es oportuna y confiable.

La evaluación es un proceso sencillo, que necesita el listado de los procesos declarados por la empresa como parte del SGSI, la revisión detallada de cada uno y una opinión crítica del auditor en cuanto a en que escala se encuentra dicho proceso.

2.3 Informe y seguimiento de la auditoría del SGSI

Concluida la revisión detallada de los controles es necesario continuar a la fase final de la auditoría, esto es avanzar en la preparación del informe de auditoría.

Es importante considerar que se debe incluir en el cronograma de trabajo un espacio de tiempo razonable para la elaboración del informe de auditoría, que dependerá de la duración total y alcance de la auditoría.

El informe de auditoría del SGSI deberá contener secciones separadas con fines específicos sugeridos con la siguiente estructura:

- Resultados de revisión del SGSI.- en la cual se deberá concluir sobre el SGSI, su estructura y la evaluación de cada uno de sus componentes.
- Resultados de revisión de los controles implementados.- en la cual se deberá concluir sobre los controles detallados que la organización ha incluido dentro de la declaración de aplicabilidad.
- Resultados de evaluación de madurez de los procesos de seguridad de la información.- en la cual se debe detallar la calificación de madurez de los procesos evaluados de seguridad de la información.

La revisión de resultados del SGSI deberá considerar evaluar cada una de las dimensiones del mismo de acuerdo al ciclo PHVA (Planificar, Hacer, Verificar y Actuar):

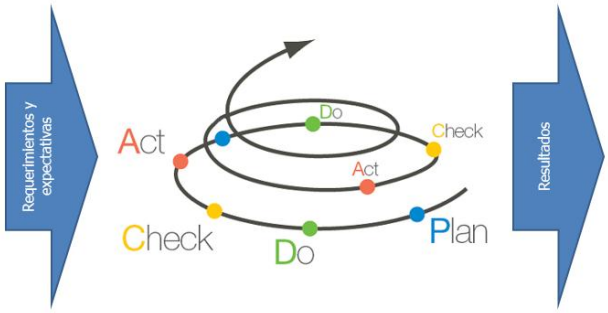


Figura 2.3 Ciclo PDCA

Y cada dimensión deberá contener una evaluación específica, a modo de ejemplo:

Planificar - Plan

El área de Seguridades no cuenta con una política de seguridad de la información, ni procedimientos, existen varios instructivos que son manejados internamente y que no existe evidencia que sean publicados o difundidos en su totalidad, además no se cuenta con un inventario de los activos críticos de la organización ni con una gestión de riesgos.

No se ha podido tener evidencia sobre actividades de planificación de la gestión de la seguridad de la información para implementar controles, evitar/corregir situaciones no deseadas y medir la operación del área.

Hacer - Do

En muchos casos no existe evidencia de la implementación de las políticas y procedimientos en toda la organización, no se tiene definido procesos de gestión que se encuentren interrelacionados con las distintas áreas de negocio de la organización, principalmente con Tecnología. La mayoría de los esfuerzos en seguridad de la información del área de Seguridades y Tecnología se enfocan en manejar los incidentes de seguridad que se presentan.

Verificar - Check

No existen evaluaciones o mediciones sobre los procesos del área de Seguridad, solo se realizan revisiones por parte de auditoría externas (“financiera”) cada 6 meses, donde se incluyen revisiones de seguridad de forma superficial revisando principalmente temas relacionados al control de accesos.

Actuar - Act

No existe evidencia de acciones correctivas o preventivas tomadas para mejorar la gestión de la seguridad de la información en base a los informes de auditoría externa o cualquier otro informe, tampoco existen un plan de mejoramiento continuo.

La revisión de los controles implementados deberá concluir sobre cada uno de los controles evaluados, a modo de ejemplo:

A.5 Política de Seguridad							
N°	Objetivo	Control	Grado de Madurez	Observación	Recomendación	Responsable de Implementación	Fecha de Implementación
1	A.5.1	5.1.1	2	Se tiene definida una política de seguridad, se han definido los objetivos y alcances generales, contiene un enunciado de la intención de la gerencia y los principios de la seguridad de la información; sin embargo no se establece un marco referencial para los objetivos de controles y los controles, tampoco se incluye la estructura de la evaluación de riesgos y la gestión de riesgos. El documento no contiene referencias a procedimientos u otros documentos, sin embargo existen una serie de instructivos (procedimientos) entregados por el área de Seguridades, muchos de los cuales se encuentran publicados en la intranet de la organización. El documento contiene una definición de las responsabilidades generales del Departamento de Seguridades Informáticas. No existe evidencia de aprobación (mediante la firma de la VP de Contraloría o el Comite Ejecutivo), publicación y comunicación (mediante talleres o charlas) del documento, en muchos casos se indicó que solo es necesarión las firmas de la Gerencias de AS y Seguridades.	Revisar, actualizar y aprobar la política de seguridad a nivel organizacional, se recomienda que la aprobación del documento no solo la de el VP de Contraloría sino un comité en donde participen todos los VP de la organización. La política de seguridad deberá contener referencia a cada unos de los dominios de la norma, así como referencia a todos los procedimientos relacionados con cada domino. Se recomienda revisar los documentos vigentes de seguridades, actualizarlos para que cumplan la función de procedimiento y aprobarlos siguiendo las mismas pautas que las políticas de seguridad. Los documentos deberán contener la siguiente estructura de verificación: elaborado por (Gerencia de AS y Seguridades), revisado por (VP de Contraloría) y aprobado por (Comité de VP de la organización). Todos los documentos generados por el área de Seguridades deberán ser aprobados, publicados y difundidos a toda la organización, se recomienda realizar talleres y/o campañas de sensibilización.	Seguridades	

Figura 2.4 Ejemplo de Informe de Auditoría

La revisión de madurez de los procesos, a modo de ejemplo:

Tabla 2 Ejemplo de Calificación de Madurez del Proceso

Dominio		Nivel de Madurez
A.5	Política de Seguridad	1
A.6	Organización de la Seguridad de la Información	2
A.7	Gestión de Activos	2
A.8	Seguridad en los Recursos Humanos	3
A.9	Seguridad Física y Ambiental	2
A.10	Gestión de Comunicaciones y Operaciones	2
A.11	Control de Acceso	1
A.12	Adquisición, Desarrollo y Mantención de Sistemas de Información	1

Como toda auditoría, los informes se generan en versión preliminar y deben ser revisados con los funcionarios responsables de la auditoría por parte de la organización.

La revisión del auditado es un paso necesario como oportunidad para revisar los hallazgos y conclusiones de la auditoría, permite lograr un aseguramiento de exactitud sobre los datos que se presentan, que las recomendaciones sean realistas, eficientes y alineadas a buena práctica y/o proyectos futuros, permite acordar espacios de tiempo para la implementación de recomendaciones y obtener ese compromiso de mejora.

La práctica sugerida para el manejo del informe de auditoría es, primero, consolidar un solo documento con sus correspondientes anexos, remitir la documentación al auditado y que se agreguen sus respuestas y/o compromisos y que este nos devuelva el documento. Con esto se manejan dos versiones del informe.

La estructura de informe va a depender de las revisiones y enfoque de la auditoría, no existen formatos específicos ni estándares. Las recomendaciones a considerar para la presentación del informe es siempre elaborar un resumen ejecutivo y adjuntar al mismo los informes técnicos obtenidos como parte de la ejecución del trabajo.

La entrega del informe final debe ser en digital y en físico, siempre con una constancia de entrega/recepción.

La implementación de las recomendaciones por parte de la empresa debe sujetarse a un plan de trabajo, el mismo que consolide los compromisos que se fueron acordando durante la revisión del/los informe(s).

Es necesario que ese plan finalmente quede bajo alguna responsabilidad de seguimiento para asegurar que se cierran las brechas identificadas, siempre considerando que el plazo de cierre de observaciones dependerá de la gravedad, inversión y esfuerzo requerido, siendo que la mejor herramienta para apalancar ese trabajo es un proyecto, declarado a la organización, con presupuesto aprobado y tiempo asignado.

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

3.1 Grado de cumplimiento en cuanto a una buena práctica

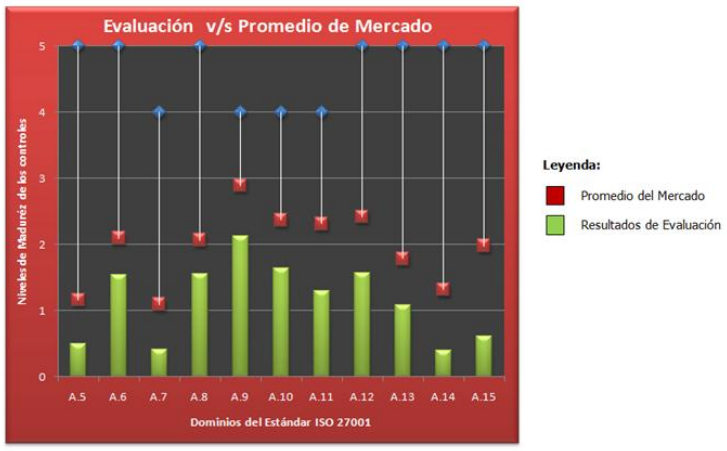
Es importante para la alta gerencia conocer el grado en el que las iniciativas realizadas por la empresa han calado y apalancado hacia buenas prácticas, finalmente si todo el mundo lo hace es porque funciona, y a estas alturas es incuestionable que una empresa que ha logrado implementar un SGSI efectivo y eficiente tiene por decantación con información mejor resguardada.

El cumplimiento del SGSI versus las buenas prácticas y estándares definidos por la organización, sin embargo no es una tarea sencilla y se debe siempre poder conocer como estamos, se debe considerar además que no hay medida entro lo bueno y lo

malo, lo que sí existe son referencias que permitirán identificar, dependiendo de varias consideraciones, cómo está la empresa en relación a otras empresas del mismo sector en otros lugares del mundo.

Con los resultados de este trabajo y obteniendo información adecuada sería posible lograr la visibilidad requerida.

El siguiente gráfico presenta un ejemplo de cómo mostrar a la alta gerencia este resultado:



Fuentes: Análisis GAP realizados durante los periodos de 2005 al 2010 en: Perú, Argentina, Chile y Colombia.
Information Security Breaches Survey - Technical Report (PRICEWATERHOUSECOOPERS)
Informe Anual de Seguridad en Instituciones Financieras (DELOITTE)
Report Security Latinoamérica 2009 (ESET)

Figura 3. 1 Ejemplo de presentación de situación de madurez de procesos

3.2 Aseguramiento independiente de la eficacia del SGSI

Con la ejecución de este trabajo en una empresa, además se tendrá el aseguramiento independiente, o una opinión externa sobre las gestiones realizadas en este tópico en concreto.

Las empresas tienen inversiones en seguridad de la información, y estar tranquilos de que esas inversiones se realizan de la forma más técnica y conveniente para la empresa sin lugar a dudas genera tranquilidad para quién autoriza los recursos y la confianza para quién solicita y ejecuta los proyectos para mejorar la seguridad de la información, además considerar que una buena evaluación dará confianza y podría abrir paso a proyectos necesarios pero que se han quedado relegados por prioridades de negocio.

3.3 Reforzamiento de áreas clave de operación del SGSI

El análisis de los dominios que se han implementado o están camino a hacerlo permitirá saber en cual los resultados han sido mejores y en cual los resultados no han sido los esperados.

En gestión, es importante tener claro que las acciones siempre tienen consecuencias, sean estas las esperadas o no, por lo tanto saber el grado de madurez de los procesos del SGSI permitirá saber si los resultados son los esperados o si se debe reforzar esfuerzos en áreas críticas que no han tenido resultados deseables, siempre considerando hacia donde queremos apuntalar.

3.4 Documentar y evidenciar la mejora continua del SGSI

Los resultados de una revisión de profundidad como la planteada, deben ser adecuadamente documentados en el SGSI ya que evidencian un esfuerzo importante de la organización hacia la mejora profunda de su SGSI y de la seguridad de la información de la empresa y permitirá además tomar mejores decisiones sobre las actividades futuras, dominios que requieren mayor esfuerzo y establecer de forma general la visión de hacia donde la alta gerencia apunta en cuanto a seguridad de la información.

CONCLUSIONES Y RECOMENDACIONES

El presente trabajo permite establecer las siguientes conclusiones:

1. Toda empresa de cualquier giro de negocio, debe cumplir requisitos de seguridad de la información, al menos los básicos, para lo cual se deberán hacer inversiones que deben tener resultados visibles y verificables, esto último siempre será una preocupación de la dirección.

2. Las revisiones de cumplimiento de buena práctica se realizan siempre contra la norma de mayor aceptación, en este caso la ISO 27001, por lo que siempre es recomendable las acciones de mejora de la seguridad de la información se emprendan considerando los requisitos de dicha norma.

3. Todo proyecto/iniciativa en la empresa se aprueba y se asignan recursos en relación a la importancia que la organización reconozca al tema, es necesario por lo tanto que se realice de forma continua comunicación de

los resultados obtenidos de las implementaciones y generar la confianza necesaria.

4. Es necesario que las actividades en seguridad de la información se alineen y estructuren en base a un SGSI, es un factor crítico de éxito en la permanencia y mantenimiento estructural de toda iniciativa de seguridad.

Las recomendaciones:

1. Dentro del presupuesto anual de la empresa se debe incluir un rubro que permita cubrir una revisión del funcionamiento del SGSI, si no es posible realizar esta tarea de forma anual se debe considerar realizarlo con frecuencia no mayor a tres años.

2. La revisión de la eficacia del SGSI debería realizarla personal externo de la compañía, salvo que exista personal calificado y que cumpla los principios de independencia.

3. Esta revisión y las actividades generadas a partir de la misma deben documentarse como parte de la mejora continua del SGSI, y asegurar que los compromisos sean cumplidos en todos los casos.

4. La evaluación de madurez en distintos momentos del tiempo permite visualizar de forma bastante sencilla la evolución del SGSI y es por lo tanto importante incluirlo siempre como parte de la revisión.

BIBLIOGRAFÍA

[1] INEN ISO/IEC. (2011). *NTE INEN-ISO/IEC 27001:2011.*

[2] ISACA. (2013). *Manual de Preparación para el examen CISA, pag. 30*

[3] ISACA. (2013). *Manual de Preparación para el examen CISA, pag. 40*

[4] ISACA. (2007). *Cobit 4.1, pag. 19.*

[5] Paez, C. (2011). *http://www.academia.edu/*. Obtenido de http://www.academia.edu/6744740/5._NIVELES_DE_MADUREZ_PARA_EL_PROCESO_DE_SEGURIDAD_DE