CAMINO A SEGUIR PARA ALCANZAR UNA CERTIFICACIÓN INTERNACIONAL BAJO LA NORMA ISO/IEC 27001:2005

Karina Del Pilar Pabón Molineros,

Unidad de Gestión de Postgrados;
Escuela Politécnica del Ejército,
Sangolquí, Ecuador
karinpabonm@hotmail.com

RESUMEN: La decisión de una organización de brindar el adecuado tratamiento a los riesgos asociados a la seguridad de su información mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) para obtener una certificación internacional; es una decisión estratégica, sustentada en el analisis de la naturaleza de la organización, el ámbito donde se desarrolla y produce, las necesidades de la empresa, sus clientes y proveedores, su situación en el mercado y el posicionamiento en el pais donde se encuentra. El trabajo a realizarse no solo debe centrarse en aplicar normas o seguir metodologías de implementación y revisión a dicho sistema de seguridad de la información, sino que debe enfocarse a como concientizar a toda la organización para que acepte este nuevo reto y se comprometa enteramente en el rol que le toca asumir. Lastimosamente este es el trabajo mas arduo por que los resultados dependen de como el recurso humano acepta las nuevas tendencias, los cambios bruscos en cuanto a gestion operativa, en como apoya y ofrece opciones para mejorar el proceso que esta cambiando y como comprende a la organización en la transicion estratégica que esta adoptando. Con este antecedente, revisaremos la situacion de una empresa estatal cuya necesidad es alcanzar una certificacion internacional bajo la norma 27001:2005, pero que despues de la estabilización de su sistema de gestión de seguridad de la información y su posterior revisión, no podía cerrar observaciones importantes que impedirían cumplir con su objetivo; el trabajo realizado muestra como el cambio de táctica para sensibilización en una empresa tan compleja surtió efecto reduciendo en un porcentaje considerable sus debilidades y asi alcanzar a la certificación internacional.

PALABRAS CLAVES: Certificación, auditoría, estructura organizacional, concienciación.

ABSTRACT: The decision of an organization to give the suitable treatment to the risks associated with the Information Security by means of the implementation of a Information Security Management System. (ISMS) to obtain an international certification; is a strategic decision sustained in the analysis of organization's nature, the area where it's develops and produces, company´s need, his clients and suppliers, his situation on the market and the positioning in de country. The work has to realize not only on applying procedure or to follow methodologies of implementation and review to Information Security Management System. In fact, must focus to the organization in order that accepts this new challenge and assume compromises in the role that has to practise. Pitifully, this one is the work mas arduous because the results depend, of how the human resource accepts the new trends, the sudden changes in the operative management, in how supports and offers options to improve the process that is changing and as understands the organization the strategic transition that is adopting. With this precedent, we will check the situation of a state company which need is to reach an international certification under the norm 27001:2005, but that after the stabilization of his Information Security Management System and his later review, could not close important observations that

would prevent to reach with his aim;The realized work shows as the change of tactics for increasing awareness in such a complex company, it supplied effect reducing in a considerable percentage his weaknesses and this way to reach to the international certification.

KEYWORDS: Certification, Audit, Organizational structure, increasing awareness.

1. INTRODUCCIÓN

“No hay nada más difícil de emprender, ni más dudoso de hacer triunfar, ni más peligroso de manejar que el introducir nuevas leyes. El innovador se transforma en enemigo de los que se beneficiaban con las leyes antiguas y no se granjea sino la amistad tibia de los que se beneficiarán con las nuevas.” (Nicolás Maquiavelo, 1513).

Después de haber investigado arduamente sobre temas de manejo de personal, ejecución de ideas e innovación empresarial, he leído muchas veces la frase citada anteriormente y cada vez me convenzo que a pesar de haber sido escrita por los años 1500 es una conclusión verdadera y aplicable aun en el siglo XXI.

En verdad, es muy fácil hacer que los seguidores desistan de las ideas de quienes los guían, muy complicado mantener y tener vigente las nuevas leyes, ya que implican sacrificio, trabajo constante e incansable.Inicio con esta meditación porque hay que reconocer que en cada realización y ejecución de proyectos siempre nos tropezaremos con serias dificultades que solo con gran valor pueden ser superadas y los cuales una vez en ejecución, la dificultad se centra en la mantención y marcha.

En base a la experiencia obtenida al desarrollar trabajos similares he palpado que es realmente sencillo aplicar para cualquier situación:

- Lo que solicita y exige una norma para la evaluacion de requisitos y controles implementados en un sistema de gestión de seguridad de la información,
- Seguir pasos establecidos y estandarizados en cuanto a validaciones sobre sistemas de gestión de seguridad de la información,

Sin embargo, lo ciertamente complicado es evaluar un SGSI con la transición que implica la gestión operativa rutinaria con los cambios que se presentan por la gestion estratégica que una empresa esta implementando. Esta transición permite visualizar factores que dificultan el curso de los proyectos desde diferentes niveles jerarquicos:

- Desmotivación y desconocimiento sobre el proyecto.
- Falta de compromiso tanto de la alta gerencia y los niveles siguientes.
- Resistencia al cambio.
- Falta de concienciación y esperanza de adquirir conocimiento sobre el tema.

Si bien estos factores son los que cualquier empresa puede experimentar al ejecutar un cambio, adaptacion y adopcion de nuevos procesos; en el presente artículo revisaremos la situación de una empresa A, de acuerdo a su naturaleza y a la manera en como fue concebida en el transcurrir del tiempo y su actual situacion.

A. Antecedentes

La empresa A es una entidad que ha sufrido cambios importantes en corto tiempo: una fusión de empresas, cambio de denominación y razon social ademas de haber sido absorbida por el estado donde se desarrolla. El negocio de la empresa son las telecomunicaciones; donde, el servicio que

genera la mayor parte de ingresos economicos se centra en la venta e instalacion de servicios de internet y datos, ademas de haber diversificado su servicios en cuanto a telefonía movil se refiere y televisión satelital. La empresa A, necesita obtener una certificación internacional para satisfacer los nuevos requerimientos del mercado, los clientes corporativos exigen con mayor frecuencia a los proveedores oferentes de servicios de internet y datos en las licitaciones, la certificación en la norma ISO/IEC 27001:2005.

La empresa A con apoyo de consultoría externa implementó un SGSI de acuerdo a las condiciones del negocio y necesidades de sus clientes. Esta implementacion se enfocó en el proceso de venta anteriormente mencionado con el objetivo de elevar los atributos del negocio basados en la información estratégica de la empresa apalancados en su misión, visión, estrategia de innovación y transformación empresarial. Ahora de acuerdo con la norma para alcanzar la certificación internacional la empresa A debe realizar a intervalos planificados Auditorías Internas a su SGSI para determinar si cumple con los requisitos de la norma ISO/IEC 27001:2005, la legislación y las regulaciones relevantes.

Inicialmente se supuso que la empresa A cumplía parcialmente con los requisitos de la Norma ISO/IEC 27001:2005.Para comprobarlo, se elaboró el plan de trabajo de auditoria interna de acuerdo con lo especificado en la cláusula seis de la norma ISO/IEC 27001:2005, se ejecutó la auditoría interna del SGSI (en dos fases por la cantidad de controles a ser revisados),y se analizaron los resultados.

Los hallazgos encontrados en las auditorias internas realizadas a la empresa A, evidenciaron que el mayor porcentaje de no conformidades indican que no cumple con los requisitos sobre capacitación, sensibilización, competencia y compromiso de la dirección, motivo para que se registre una recomendación de no certificación internacional por afectar directamente a los requisitos obligatorios de la norma. Ocho meses antes la consultora externa habia realizado una pre auditoría y habia identificado los mismos hallazgos y elaborado un plan de acción para el cierre de estos a los cuales se habia dado tratamiento por parte de los responsables del proyecto en la empresa A. Ahora el cuestionamiento es:

¿Por qué a pesar de haber sido cerradas las observaciones encontradas con la consultora externa se siguen presentando los hallazgos más importantes al cumplir con el requisito seis de la norma?;Y mas aún después de un tratamiento de ocho meses para el cierre de las mismas.

B. Situación actual

La empresa A en un tiempo de dos años realizó cambios en su estructura organizacional, actualmente la empresa A es el resultado de una fusión con dos empresa de naturaleza distinta, la primera de ellas tradicional con varios años en el mercado, con servicios identicos a la empresa A y en si una estructura similar, organicamente sin mucha dificultad de adaptación, salvo por el personal que por su ubicación geográfica diversaban en su manera de proceder, actuar y por ende de trabajar. La segunda empresa, dinámica y activa por la naturaleza de sus servicios; benefició a la empresa A en la ampliación de su portafolio de servicios, incrementando su posicionamiento en el mercado. La variabilidad entre esta organización y la empresa A, radica igualmente en el personal el cual por pertenecer a una empresa joven e innovadora con pocos años en el mercado diferia en conocimiento y años con los colaboradores de la empresa A.

Como observamos en muy poco tiempo la empresa A sufrió cambios importantes con poco tiempo de adaptación para sus colaboradores. La unión de dos o mas sociedades preexistentes, en la que una puede subordinar a la otra o pueden obtener el mismo grado de participación bajo una nueva sociedad, implicó el desarrollo e implementación de proyectos en plazos muy cortos para la adaptabilidad del personal con la nueva situación.

Este proceso de transformación, transicion e integración que facilita oportunidades y avances para el crecimiento y fortalecimiento de una empresa, tambien trae un alto riesgo de amenazas para la misma; es así como respuestas asociadas a estas situaciones generan: caos, desorganizacion, cambios radicales y miedos.

La unión de dos o mas culturas organizacionales podrían ser en ciertos casos contraproducentes sino son tratadas de la forma adecuada; el clima organizacional podria verse afectado si la sensibilización de la situación no fue difundida a tiempo, e incluso podría resarcirse hasta varios años despues, mientras no se logre el compromiso del personal que aun no acoge este cambio, y sigue sintiendo en peligro su estabilidad, su modo de trabajar rutinario con su horario inflexible, sin aportar un esfuerzo adicional en pro a la mejora de la situacion actual.

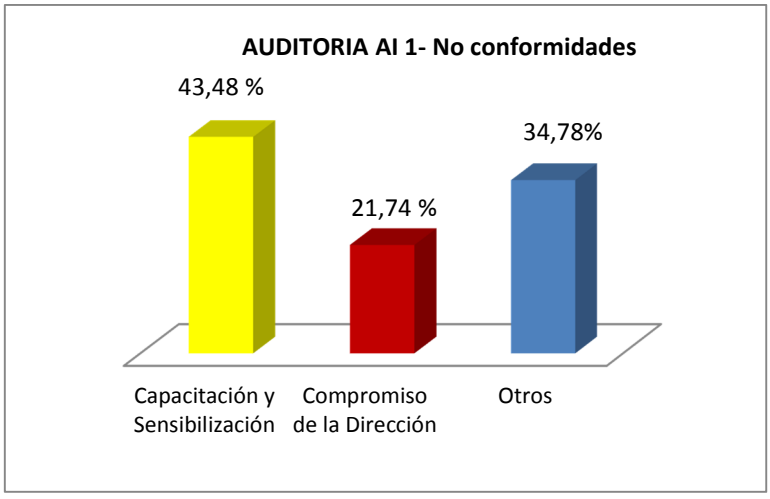
2. METODOLOGÍA

Para iniciar con el presente estudio, cabe indicar que se ha utilizado una metodología propia de la empresa A y demás herramientas como es el ensayo de prueba y error que permitieron obtener los resultados esperados y así cubrir las necesidades de la empresa A.
Los resultados a ser revisados en esta parte, son de acuerdo a una evaluación real realizada de la cual parte este artículo.
En las dos fases de la auditoría interna realizada al SGSI de la empresa A, la mayor parte de no conformidades detectadas se centran en el tema de capacitación, sensibilización, competencia y compromiso de la dirección. Revisemos los resultados obtenidos de la primera auditoría (en adelante AI) realizada en inicios del año 2013, mes de febrero:

De los hallazgos encontrados en AI1, el mayor porcentaje atenta contra el requisito 5.2.2 Capacitación, sensibilización y competencia, seguido en un menor pero importante porcentaje con el requisito 5.1 Compromiso de la Dirección, el restante es la sumatoria de requisitos y controles los cuales abarcan no conformidades menores y oportunidades de mejora que no afectan mayoritariamente a la recomendación de certificación por lo cual no seran objeto de nuestro estudio.

Las barras amarillas y rojas nos indican el porcentaje de incidencia con respecto a los puntos mencionados, la problemática se centran en que este porcentaje no ha disminuido con respecto a las no conformidades detectadas por la consultora externa.

GRÁFICO 1. No conformidades AI1



En la evaluación realizada, como experiencia personal pude observar que en un porcentaje del 80% los entrevistados no se encontraban comprometidos con su rol en el proceso a ser auditado.

De las veinte entrevistas realizadas, pude registrar al menos una reflexión en el ambito personal del colaborador; los entrevistados no estaban dando la debida importancia al tema de seguridad de la información, incluso no le daban importancia a la auditoría misma, comprometiendola a faltas, tardanzas e incluso cancelaciones. Es decir, con un SGSI implementado hace mas de un año, con una auditoria realizada para evaluar el estado situacional de la empresa, con planes de accion ejecutados y observaciones cerradas, aun la empresa A no estaba conciente sobre lo que significaba tener un sistema de gestion de seguridad de la información y el trabajo que conllevaba mantener el mismo.

Con tantas observaciones sobre el tema surge la cuestión: ¿Qué estaba sucediendo?, la respuesta se la obtuvo en la presentación del informe de auditoría, muchos representantes de la alta dirección no asistieron en la exposición realizada.

El objetivo despues de cumplir con el requisito seis de la norma era proponer a la empresa A para una evaluación externa y asi alcanzarla certificación internacional ISO 27001:2005.

Luego de la evaluación realizada en AI1, la empresa de certificación se presentó para realizar una auditoría externa de primera fase a la empresa A, la espectativa era pasar esta evaluación de en la primera fase pero lastimosamente salieron a la luz estas falencias y la recomendación del auditor externo fue cerrar las mismas observaciones ya determinadas. El hallazgo encontrado por la empresa de certificación fue la no recomendación para la certificación internacional.

A. Ejecución de planes de acción

Después de estas auditorias, el plan de acción se enfocó en su mayoría en planes de capacitación, sensibilización y concienciación. El método a ser utilizado fue el tradicional: plan de capacitaciónes ejecutadas en semanas programadas a los cuales el personal debía asistir para instruirse sobre temas de seguridad de la informacion; lastimosamente despues de la primera semana de capacitaciones nos dimos cuenta al revisar las actas de asistencias capacitaciones y según la presencia de los colaboradores in situ, que para la realidad como empresa no se estaba utilizando el metodo correcto para concienzar a los colaboradores sobre temas de seguridad, en la semana uno de capacitaciones asistieron 55 colaboradores de los 300 involucrados en este proceso.

La empresa A, presta varios servicios y cada vez innova con nuevos productos para sus clientes, demandando a su personal un trabajo constante con resultados inmediatos para satisfacer a sus clientes, encontrandose esta exigencia en todas las áreas de la empresa: sean las técnicas, de sistemas, de servicio al cliente, o las de operación.

Al analizar el por qué la falta de asistencia a las capacitaciones se encontró lo sigueinte:

1. **Falta de tiempo por parte de los colaboradores**: el trabajo bajo presión no les permite ausentarse de su puesto de trabajo por algo tan trivial como una capacitación.

2. **Falta de interes sobre el tema de seguridad de la información**: el personal por desconocimiento no deseaba saber las nuevas tendencias sobre seguridad de la información; “por qué modificar mi forma de cuidar la información si siempre he trabajado así y no ha sucedido nada?. Este tema es delicado por que implica temas como:

   - El perfil del colaborador en cuanto a educación se refiere,

   - Los años de prestación de servicios por temas de fusión de empresas,

   - Colaboradores con resistencia al cambio.

3. **Falta de colaboración de jefaturas**: el trabajo excesivo que se tiene en ciertas áreas de la empresa A, los turnos rotativos, la exigencia de atención 7x24, causa que no todos los colaboradores puedan asistir a las capacitaciones impartidas. Las opciones de las jefaturas fueron: el colaborador que desea puede asistir fuera de los horarios de trabajo o solamente se limitaron a enviar uno o dos representantes del grupo de trabajo.

4. **Lugar donde se realiza la capacitación**: el lugar que la empresa A destina para las capacitaciones es bastante alejado de los lugares de trabajo de los colaboradores por lo que el traslado y el regreso a las oficinas es dificil, lo que genera que los colaboradores opten por no asistir.

5. **Cantidad de horas de capacitación**: para muchos asistir a una capacitación de cuatro horas es bastante tedioso y mas aún si es obligatorio.

Tras haber realizado este análisis, de manera reactiva y de acuerdo a las situaciones encontradas inmediatamente se comenzó con la difusión de los temas de seguridad de la información explotando los recursos que la empresa posee, para de esta manera intentar cerrar las novedades mencionadas, y se lo hizo asi:

1. **Por la falta de tiempo de los colaboradores:** Por un medio de difusion masivo que la empresa posee y que llega a nivel nacional, se difundió pequeños tips de seguridad de la información, el medio de difusión utilizado fue el correo electrónico. Cuando se comenzó con la campaña, se enviaban diariamente tips de seguridad de la información en un periodo de aproximadamente dos meses. Actualmente la campaña continua y se encuentra en el calendario de difusion del área encargada de la comunicación en la empresa, ahora la difusión se realiza los martes de cada mes.

2. **Falta de interes sobre el tema de seguridad de la información:** con las difusiones realizadas por el canal de comunicación interno, se generó interes incluso con los colaboradores mas reacios, el hecho de revisar los tips sobre canales oficiales y masivos, causó que del grupo detectado en un 40% se inclinarán a conocer mas sobre el tema.

3. **Falta de colaboración de jefaturas**: El hecho de poder recibir tips de información en el mismo lugar de trabajo, sin dejar de realizar las tareas diarias, facilitó a las jefaturas el inconveniente de ausentar recursos y retardar la atención requerida en el área. Para poder reforzar estos temas se comenzó a colocar material en carteleras de las diferentes areas y jefaturas sobre seguridad de la información, su politica y tips adicionales para que el colaborador al ingresar o salir de las instalaciones pueda leer y recordar lo revisado a través del canal de difusión. Tambien se crearon ayudas memoria publicadas en el sistema de gestión documental de la empresa y del cual la alta dirección tenia el deber de difundir entre los colaboradores.

4. **Lugar donde se realiza la capacitación:** en algunos casos fue necesario formar grupos de capacitacion dirigidos para cada área por periodos determinados, al final se determinó un nuevo sitio oficial para capacitación, el cual se centró en las instalaciones donde se encontraba el mayor número de ausentismos.

5. **Cantidad de horas de capacitación:** el tiempo de capacitación fue reducido a dos horas realizandose por fases, obviamente se ampliaron las semanas de capacitación y la asistencia de colaboradores fue consideramente alta.

Todo este plan de acción tardó en ejecutarse entre cuatro y cinco meses incluyendo todos los temas de gestión interna que se debe realizar en la empresa A para oficializar tanto las difusiones por medios masivos como las capacitaciones realizadas.

Para conocer si en verdad surtió efecto la gestión, se realizó una una evaluación de efectividad de la capacitación. Esta revisión volvió a demostrar que aún no se podía cerrar con éxito las observaciones de capacitación, sensibilización y concienciación. Sin embargo, con satisfacción se pudo mostrar que se habian resuelto en un 75% el tema de capacitación, sensibilizacion y competencia al igual que el compromiso de la dirección, pero aun seguia siendo un inconveniente que atentaría a una recomendación de no certificación. Todavía se tenía que buscar formas de concienzar sobre seguridad de la información a los colaboradores de la empresa A.

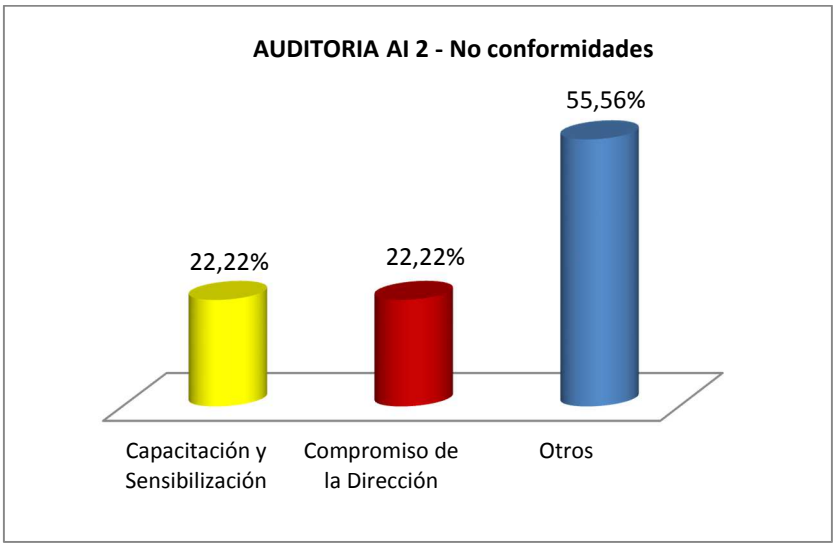
Con el apoyo de la alta dirección y su disposición se procedió a generar una capacitación obligatoria la cual debía ser aprobada por todos los involucrados en el proceso del Sistema de Gestión de Seguridad de la Información en un tiempo determinado.

Este curso realizado por el canal interno oficial de capacitaciones que posee la empresa A, tuvo como estrategia enviar un mail personalizado a cada empleado para que ejecute el curso de seguridad de la información de manera obligatoria, la no ejecución de la misma seria sancionada ejecutando el reglamento interno de la empresa A.

EVALUACIÓN DE RESULTADOS

Para evaluar sobre todo el trabajo realizado en los meses anteriores al cerrar las no confomidades mencionadas, se realizó la segunda auditoria a la empresa A (en adelante AI2) en la primera semana del mes de septiembre, realizando la revision de la misma se encontró:

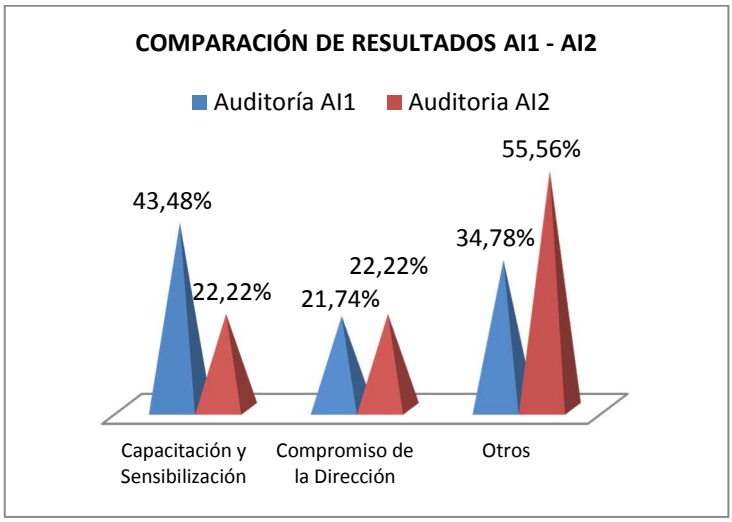
GRÁFICO 2. No conformidades AI2



El tema de preocupación sobre Capacitacion, Sensibilizacion y Competencia llegó al 22% de los hallazgos encontrados y en idéntico porcentaje el tema de Compromiso de la Dirección, evidenciando que se ha reducido en mas del 50% las no conformidades encontradas en AI1. Al realizar una comparación gráfica de los resultados obtenidos en la auditoría de AI1 y AI2, se puede ver con mas claridad la diferencia en el cierre de no confomidades con respecto a este tema.

La gráfica indica que la incidencia que venía repitiéndose por casi un año fue superada con gran éxito al culminar la auditoria interna AI2 como cumplimiento del requisito número seis de la norma. Si bien en la segunda auditoría se registraron hallazgos con referencia a estos requisitos, fueron en menor grado y tratables para llegar a la auditoría externa a realizarse a inicios del mes de octubre.

GRÁFICO 3. Comparación de Resultados entre AI1 y AI2



Al someterse la empresa A a la auditoría externa para obtener la certificación, corría el riesgo de que estos hallazgos sean encontrados por el auditor de certificación, tema preocupante para la empresa A por lo cual para cerrar estas observaciones la organización tuvo que trabajar arduamente durante tres semanas sobre temas de capacitación y difusión de procedimientos. Por supuesto estas acciones se lograron con el apoyo de la alta dirección ya que los mismos por su importancia debieron ser de cumplimiento obligatorio.

La empresa de certificación, en la segunda revisión realizada determinó que la empresa A, tenía un sistema de gestion de seguridad de la información, eficaz y efectivo en la operación y gestión de su SGSI, con compromiso de todos sus colaboradores y la alta dirección; por lo tanto, la certificación internacional fue otorgada.

3. TRABAJOS RELACIONADOS

Con respecto a la implementación y revisión de sistemas de seguridad de la información, existe un sin número de trabajos realizados específicamente para cada empresa ó institución que se ha visto en la necesidad de implementar proyectos de esta índole, por consiguiente, en cuanto a información existe mucha, lo importante es tener la habilidad para analizar y distinguir que se puede aplicar de acuerdo a las necesidades del caso de estudio planteado.

4. CONCLUSIONES Y TRABAJOS FUTUROS

Al realizar las auditorìas internas, la mayor dificultad que se encontró; fue la falta de colaboración de los empleados, los cuales no actúan mientras no tengan una motivación que en este caso se presentó como una disposición de cumplimiento obligatorio. Es imprescindible, trabajar no solo por el objetivo de mantener un Sistema de Gestión de Seguridad de la Información o por que las disposiciones indican o no una forma de actuar determinada. El trabajo debe reforzarse en concientizar a los colaboradores del significado de crecer como empresa y prestar servicios de calidad en un tiempo oportuno y la seguridad.

El conocer el camino que emprende la empresa para posicionarse en el mercado, implica un orden, disciplina, sacrificio, trabajo arduo e incansable, que solo se logra con el compromiso de todos los que forman parte de la organización. El camino a seguir es lograr un cambio de mentalidad o cultura organizacional donde se entienda que sin el esfuerzo propio, el avance y crecimiento tardará aún más, porque con el consentimiento o no de todos, el cambio vendrá.

Al aplicar una táctica diferente en la manera de difundir los conceptos clave sobre seguridad de la información y sea una disposición de cumplimiento obligatorio, se generó una clara mejora en los cierres de observaciones sobre el tema de capacitación y compromiso de la concluyendo que los métodos sugeridos sobre aplicaciones de planes de acción deben variar de acuerdo a la naturaleza de la organización, su situación actual, y las exigencias que requiere para mantenerse en el mercado.

Cada vez existen más riesgos de seguridad y con impacto mayor, por lo que se debe estar atento a las nuevas tendencias, siendo alternativos con la manera de proceder y responder con prudencia a los sucesos repentinos que puedan dañar los activos. La seguridad de la información de una empresa la hacen todos sus colaboradores, comenzando por la alta dirección, y sus niveles. Es importante que se recuerde que la cadena de la seguridad de la información se rompe por medio del eslabón más débil.

Todos podemos crear y trasmitir conciencia, como miembros de un equipo, como parte de una familia, el éxito está en prepararnos, actualizarnos e intentar caminar a la velocidad que lo hace el mundo.

5. REFERENCIAS BIBLIOGRÁFICAS

Pabón Molineros, K. P. (Diciembre 2013). Auditoría interna al SGSI de la CNT E.P. para el proceso de venta e instalación de productos y servicios de datos e internet para clientes corporativos en el D.M.Q. Quito, Ecuador.