Desde el sistema de gestión de calidad a la seguridad de la información propuesta en ISO 27001:

Gap analysis en una empresa de transporte

García, Marcelo Adrián[1y2], Masclef, María Alejandra[1y3]

[1]Instituto de Administración - Facultad de Ciencias Económicas – U. N. Tucumán
[2]mgarcia@face.unt.edu.ar, [3]alema@webmail.unt.edu.ar

Resumen. La información de una organización constituye un activo valioso y vulnerable. Un ataque puede comprometerla total o parcialmente y afectar su disponibilidad, integridad y/o confidencialidad, causando retrasos y un alto costo económico y reputacional para la compañía. Es por ello, que la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) contribuiría con el propósito de proteger la información y los activos informáticos relacionados.

El objetivo de este trabajo es analizar el estado actual del Sistema de Gestión (SG), certificado por IRAM – ISO 9001 en calidad (SGC), implementado en una empresa dedicada a la comercialización de productos químicos para la industria, ubicada en la provincia de Tucumán, Argentina. A partir de ello, se realizará un estudio de tipo exploratorio y descriptivo, analizando los requerimientos que adicionalmente debería cumplir la organización para certificar su SG en el marco de ISO 27001 (requisitos para la implementación de un SGSI).

Cabe destacar, que las normas mencionadas cuentan con una estructura de alto nivel con apartados de títulos idénticos, términos comunes y, entre otros, definiciones esenciales indicadas en el anexo SL de la Directiva ISO/IEC, parte 1, "Consolidated ISO Supplement", lo que hace que su implementación conjunta sea compatible.

A partir de la solicitud por parte de la empresa de incorporar controles de seguridad en sus procesos críticos de negocios, se considera que la implementación de un sistema de gestión que cumpla simultáneamente con requerimientos de Calidad y Seguridad de la Información, se presenta como una propuesta de extensión factible para la entidad objeto de estudio. Ello contribuiría a la mejora continua de sus procesos y a la definición de un umbral aceptable de riesgo asociado a la utilización de sus activos de información.

Palabras clave: Seguridad de la Información – Sistema de Gestión – ISO 27001

1 INTRODUCCIÓN E IMPORTANCIA DE LA ACTIVIDAD

Un sistema de gestión es una herramienta que le permite a las organizaciones obtener un óptimo y ordenado desempeño y mejorar su posicionamiento en el mercado. Además, constituye una importante fuente de información, para profesionales de cualquier

actividad económica. En él se establece la estructura, los roles y responsabilidades, una adecuada planificación, operación, políticas y reglas. Asimismo, se definen las creencias, objetivos y procesos necesarios para lograr las metas establecidas en la estrategia corporativa.

Las normas ISO que abordan los “Sistemas de Gestión” cuentan con una estructura de alto nivel con apartados de títulos idénticos, términos comunes y, entre otros, definiciones esenciales indicadas en el anexo SL de la Directiva ISO/IEC, parte 1, “Consolidated ISO Supplement”, lo que hace que la implementación conjunta de cualquiera de ellos sea compatible.

Considerando que la información de una organización constituye un activo valioso y vulnerable. Un ataque puede comprometerla total o parcialmente y afectar su disponibilidad, integridad y/o confidencialidad, causando retrasos y un alto costo económico y reputacional para la compañía.

El SGC que se encuentra implementado se presenta como el punto de partida para poner en marcha un SGSI, ambos integrados. Esta situación contribuiría con el propósito de proteger la información y los activos informáticos relacionados, simultáneamente con el cumplimiento de los objetivos propuestos por la dirección de la empresa.

A partir de la solicitud por parte de la compañía de incorporar controles de seguridad en sus procesos críticos de negocios, la implementación anteriormente descripta se presenta como una experiencia de vinculación con el medio económico local.

2 IDENTIFICACIÓN DE OBJETIVOS

2.1 Objetivo General

Realizar un estudio de los requerimientos de seguridad de la información que debe cumplimentar una empresa comercial ubicada en la provincia de Tucumán, en base al marco de cumplimiento ISO 27001 (SGSI), tomando como punto de partida su SGC implementado.

2.2 2.2. Objetivos específicos

1. Efectuar un relevamiento de los requisitos que cumple la organización para la implementación de un SGSI, considerando que actualmente posee un Sistema de Gestión certificado en Calidad.
2. Identificar las acciones que deberían implementarse para poner en marcha un SGSI acorde a lo requerido en la norma ISO 27001.
3. Presentar a la organización objeto de estudio conclusiones respecto a la implementación de un SG integrado que cumpla requisitos de Calidad y Seguridad de la Información.

3 PLANIFICACIÓN DE LA INTERVENCIÓN Y DE SU SEGUIMIENTO

El presente trabajo se realiza en el ámbito de una empresa, cuyo objeto social es la comercialización de productos químicos para la industria. La misma posee un Sistema de Gestión de Calidad certificado por IRAM – ISO 9001. Sus oficinas administrativas y centro de almacenamiento y distribución se encuentran ubicados en la provincia de Tucumán, desde donde ofrece sus productos y servicios en jurisdicciones del centro y norte del país.

En ella, se efectuó un análisis de los requerimientos necesarios para implementar un único Sistema de Gestión que cumpla con los requisitos de Calidad y de Seguridad de la Información, considerando los marcos normativos de ISO 9001 e ISO 27001 respectivamente.

Se tomó como modelo estándares internacionales para la implementación del SG.

Los estándares surgen a partir de mejores prácticas y son utilizados como herramientas estratégicas para intentar reducir costos, minimizar errores; así como aumentar la productividad dentro de las organizaciones. La selección de un estándar de carácter internacional brinda beneficios adicionales, ya que permite posicionarse en un marco comparativo a nivel mundial.

Las actividades para dar cumplimiento a los objetivos propuestos fueron las siguiente:

1. Definir y entender, en toda su dimensión teórica, el concepto de Sistema de Gestión. Para ello, se profundizaron los siguientes conceptos:

- Activos de la Información
- Seguridad de la Información (SI)
- Relación de la Seguridad de la Información con la gestión de negocios
- Sistema de Gestión
- Sistema de Gestión de Seguridad de la Información
- Evaluación de la Seguridad de la Información
- Alcance de la Seguridad de la Información
- Diseño e Implementación de un SGSI
- Responsabilidades de la Dirección
- Requisitos de documentación de ISO / IEC 27001
- Cuerpo normativo común entre ISO 27001 e ISO 9001

2. Efectuar un relevamiento de los requisitos que actualmente cumple la organización para la implementación de un SGSI, por contar con un SGC
3. Identificar acciones y controles de seguridad de la información que deberían implementarse para poner en marcha un SGSI acorde a lo requerido en ISO 27001
4. Clasificar y ordenar de la información relevada
5. Desarrollar de conclusiones

4 ANÁLISIS DE RESULTADOS

Los principales resultados del análisis realizado en la empresa objeto de estudio, se detallan a continuación.

a. Contexto de la organización

- Comprensión de la organización y su contexto
- Necesidades y expectativas de las partes interesadas
- Alcance del SGSI

Teniendo en cuenta la primera fase del "Ciclo de Deming", la cual implica "planificar", se hace referencia a la importancia de conocer la organización y el contexto en el cual está inserta. Deben identificarse las necesidades y expectativas de las partes interesadas, el alcance y las particularidades del SGSI.

La empresa analizada, efectúa un análisis periódico para la comprensión de su funcionamiento y contexto, a través de la herramienta FODA.

En cuanto a la identificación de "partes interesadas" tiene un fuerte enfoque en la calidad. Por lo tanto, deberían identificarse aspectos que intervengan en la seguridad de la información.

Se verifica que posee definido un alcance para su Sistema de Gestión. Pero por su naturaleza, el mismo difiere a lo solicitado por ISO 27001, pues cada norma añade requisitos específicos. Por lo tanto, debería efectuarse una adecuación de este punto, teniendo en cuenta el mapa de interacción de procesos, para cumplimentar apropiadamente la exigencia.

b. Liderazgo

- Liderazgo y compromiso
- Cultura de Seguridad de la Información
- Política de Seguridad de la Información
- Roles, responsabilidades y autoridades

La norma ISO 27001 indica que la alta dirección debe ejercer liderazgo y compromiso respecto a la implementación y seguimiento del SGSI. Para ello, debe tenerse en consideración la cultura organizacional y los recursos disponibles para dar cumplimiento a los objetivos de seguridad propuestos.

Se comprueba que la organización objeto de estudio tiene definida una "Política de Calidad". Por lo tanto, deberá efectuar una adecuación de la existente para dar cumplimiento conjuntamente a los requisitos de Calidad y de Seguridad de la Información; o en su defecto establecer una política independiente y específica a tal fin.

En el mismo sentido, para realizar un efectivo gobierno y gestión de la SI, es necesario contar con una adecuada estructura, dentro de la cual deben definirse perfiles, roles y funciones. Cabe destacar que, dependiendo de la magnitud y las características de la organización, el tipo de estructura y la cadena de mandos podrían diferir. A tal

fin, se propuso, un perfil de puesto para el "Responsable de Gestión de la Seguridad de la Información" (CISO).

c. Planificación

- Riesgo
- Vulnerabilidad
- Amenaza
- Acciones para tratar el riesgo
- Objetivos de SI y planificación para los logros

Este capítulo trata uno de los requerimientos centrales del SGSI, el cual es la gestión de riesgos. Además, dentro de la planificación aborda la definición de los objetivos de seguridad de la información, para los que se deben definir acciones, recursos y responsables.

Se verifica que la organización posee documentos en donde se efectúa una evaluación de riesgos: Análisis de Contexto – FODA (contexto); Partes Interesadas (contexto); Matriz de riesgos de proceso (operacional); Planilla de Seguimiento de reclamos, desvíos y acciones correctivas.

Sin embargo, para cumplimentar lo requerido en ISO 27001, se deberá efectuar una evaluación de los riesgos que afectan específicamente a la seguridad de la información. En este sentido, deberá confeccionarse la "declaración de aplicabilidad" de dichos controles. Asimismo, sería recomendable la implementación de una técnica específica para la gestión de riesgo que se base en un estándar internacional, como ser ISO 31000 o ISO 27005.

Por otra parte, se evidencia que la empresa analizada no tiene establecidos objetivos de seguridad de la información, por lo que deberá abordarse esta situación.

d. Soporte

- Recursos
- Competencia
- Concientización
- Comunicación
- Información documentada

La norma antes mencionada aborda cuestiones relacionadas a los recursos necesarios para el correcto funcionamiento de un SGSI, las competencias necesarias y la concientización requerida. Además, describe los requisitos que deben estar documentados respecto a los controles de la información.

En base a lo expuesto, la empresa debería identificar los recursos necesarios para la implementación de un SGSI (teniendo en cuenta el alcance previamente definido).

Se observa que no cuenta con personal suficiente en el ámbito de la seguridad de la Información. Sin embargo, se verifica la existencia de recursos materiales y tecnológicos adecuados para la realización de las actividades laborales que se llevan a cabo.

Debería hacerse una readecuación de la estructura y sus perfiles de puesto, para dar cumplimiento a los requisitos de seguridad de la información que plantea ISO 27001.

También correspondería definir procedimientos específicos vinculados a la temática tratada en el presente.

Se comprueba que la empresa cuenta con un "Plan Anual de Capacitaciones" y un "Procedimiento de Inducción". Actualmente no se realizan actividades relacionadas a seguridad de la información. Las mismas están enfocadas a calidad y seguridad e higiene laboral. Pero pueden utilizarse estas herramientas para cumplimentar esta exigencia.

Se planifican reuniones quincenales, en donde se tratan temas relacionados al funcionamiento del sistema de gestión, llevándose un registro, a través de minutas de reunión, de los temas abordados en cada una de ellas. En el orden del día, podrían incluirse cuestiones relacionadas a la seguridad de la información.

En cuanto a la comunicación de lo normado, se observa que en las oficinas está expuesta la "Política de Calidad" y los procedimientos están accesibles para el personal en un repositorio compartido. Lo mismo debería realizarse para los documentos del SGSI.

e. Operación

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requerimientos de seguridad de la información, las acciones para tratar los riesgos y las oportunidades. Además, deben planificarse las actividades necesarias para alcanzar los objetivos de seguridad propuestos. Todo esto debe estar adecuadamente documentado, para evidenciar las acciones efectuadas a tal fin.

Es por ello que la organización debe realizar un control de los desvíos respecto a la planificación anual efectuada, ejecutando las acciones correctivas que sean necesarias para evitar cualquier resultado negativo. También deben controlarse los procesos tercerizados.

Deben definirse la periodicidad de las evaluaciones de riesgo e implementar un plan para tratar aquellos que se hayan identificado.

Lo indicado en este apartado tiene que ser completamente desarrollado por la organización, en lo que respecta a seguridad de la información. Cabe destacar que la empresa efectúa evaluaciones de riesgo relacionadas a calidad, contexto, partes interesadas y riesgo de proceso, llevando un registro y efectuando un seguimiento de los desvíos detectados.

f. Evaluación de desempeño

- Seguimiento, medición y evaluación
- Auditoría interna
- Revisión por parte de la Dirección

ISO 27001 solicita evaluar el desempeño de la seguridad de la información y del SGSI. Encontramos aquí cuestiones de análisis y evaluación, revisión por la dirección y auditorías internas.

Se observa que la empresa cuenta con un "Plan Operativo Anual", en donde se plasman los indicadores de gestión de cada uno de los aspectos solicitados para su Sistema de Gestión.

Además, cuentan con un documento llamado “Indicadores de Gestión”, en donde se muestran los resultados de cada una de las métricas, su composición y gráficos ilustrativos. Para cumplimentar lo indicado en ISO 27001, se deberán diseñar indicadores y métricas específicas de seguridad de la información.

Se observa que la organización efectúa auditorías internas periódicas y cuenta con archivos documentales para dar cumplimiento a este requerimiento.

Se evidencia también que confecciona anualmente un documento que aborda la “Revisión por parte de la Dirección”. En el mismo sentido, deberán incluirse cuestiones relacionadas a seguridad de la información.

g. Mejora

- No conformidad y acción correctiva
- Mejora continua

Tomando nuevamente como referencia el “Ciclo de Deming”, el último capítulo normativo de ISO 27001, es el que tiene una mayor vinculación con la etapa “actuar”. En este apartado se abordarán los requisitos de las “no conformidades” y “acciones correctivas”, los cuales están relacionados con la mejora continua.

Se corroboró la confección de una “Planilla de Seguimiento de Reclamos, Desvíos y Acciones Correctivas”, en donde se efectúa un control y seguimiento de todos estos aspectos. En la misma se identifica el desvío y se efectúa su correspondiente tratamiento, seguimiento, evaluación de eficacia y riesgo. Esta misma herramienta debería utilizarse para el registro de los desvíos relacionados a ISO 27001.

5 CONCLUSIONES

En el presente trabajo se desarrolló un estudio comparativo sobre los postulados que plantea la gestión de la seguridad de la Información, con el objetivo de entender las implicancias que conlleva la implementación, seguimiento y control de un SGSI. Esto permitió evidenciar la relevancia de la seguridad informática en las organizaciones actuales y determinar la relación de esta disciplina con la gestión de negocios.

Posteriormente, se efectuó un análisis del estado actual del Sistema de Gestión, certificado por IRAM – ISO 9001 en calidad, de una empresa dedicada a la comercialización de productos químicos para la industria, ubicada en la provincia de Tucumán, Argentina. A partir de esta primera evaluación, se realizó un estudio de tipo exploratorio y descriptivo, analizando los requerimientos de su sistema de gestión que adicionalmente debería cumplir la organización para dar cumplimiento a las exigencias de seguridad de la información.

Se realizó un relevamiento de los requisitos que actualmente se cumplen, debido a que el SGC cuenta con una estructura común de alto nivel compatible con un SGSI. Luego se identificaron las acciones y controles de seguridad que deberían implementarse, para dar cumplimiento a lo indicado en ISO 27001. En este sentido, se observa que un número considerable de requerimientos actualmente están siendo cumplimentados y otros podrían ser llevadas reutilizando herramientas implementadas como, por

ejemplo: análisis de contexto, capacitaciones, auditorías, entre otros. Si existiesen variaciones en un mismo procedimiento a fin de dar cumplimiento a ambos *framework*, deberá indicarse la situación en el documento destinado a tal fin.

Por lo anteriormente expresado, se pudo corroborar que existen puntos en común entre los dos estándares analizados, por lo que se presenta una oportunidad de integración. Sin embargo, se evidencian diferencias que deben tenerse en cuenta, especificándose las cláusulas que se están cumpliendo de cada estándar.

Se hace hincapié en la importancia de la evaluación y gestión del riesgo para una adecuada dirección estratégica del negocio, lo que contribuiría a evitar incidentes que comprometan la confidencialidad, integridad y/o disponibilidad de la información y otorgaría confianza a los *stakeholders*, demostrando que los riesgos identificados se gestionan apropiadamente.

También, se recomienda la aplicación de los controles organizacionales, de personas, físicos y tecnológicos que propone el "Anexo A" de la norma ISO 27001 y se planifiquen auditorías internas periódicas que monitoreen su adecuado cumplimiento y los controles por oposición que deberían estar previstos en el diseño de los procedimientos de trabajo.

Se considera que la puesta en marcha de un sistema de gestión integrado que cumpla con requisitos de calidad y seguridad de la información, es una propuesta factible de aplicar en la entidad analizada, agregando valor y contribuyendo a la mejora continua de sus procesos de negocio. Para ello, se requerirá la asignación de mayores recursos económicos y humanos para su sostenimiento en el tiempo.

Asimismo, es aconsejable que se designe un responsable idóneo para liderar el sistema de gestión integrado; se incorporen a este todas las operaciones de la empresa y se fomenten actividades para lograr el compromiso de sus miembros y de la dirección de la compañía.

Finalmente se hace énfasis en que aquellas personas que tienen a su cargo la gestión del ente deben considerar a la seguridad de la información en el diseño de los procesos de negocios, sistemas de información y controles.

6 REFERENCIAS BIBLIOGRÁFICAS

1. Baca Urbina, G. (2016). *Introducción a la Seguridad Informática*. Grupo Editorial Patria.
2. Cano M., J. J. (2013). *Inseguridad de la Información: Una visión estratégica*. Alfaomega.
3. Deloitte. (s.f.). *¿Qué es el gobierno corporativo? Transparencia y confianza* https://www2.deloitte.com/es/es/pages/governance-risk-and-compliance/articles/que-es-el-gobierno-corporativo.html
4. Escuela Europea de Excelencia. (11 de octubre de 2016). *¿Cómo integrar las normas ISO 9001 e ISO 27001? Obtenido de Nuevas Normas ISO*: https://www.nueva-iso-9001-2015.com/2016/10/integrar-normas-iso-9001-e-iso-27001/
5. INCIBE (s.f). *Políticas de seguridad para la pyme*. https://www.incibe.es/protege-tu-empresa/herramientas/politicas
6. INTECO (s.f.). *Implementación de un SGSI en la empresa*. https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf
7. Instituto Argentino de Normalización y Certificación (2015). Norma ISO 9001: Sistemas de Gestión de Calidad. Subcomité de Sistemas de Gestión de Calidad.

8. Instituto Argentino de Normalización y Certificación (2021). Norma ISO 27002: Tecnología de la información. Técnicas de seguridad. Código de buenas prácticas para los controles de la seguridad de la información.
9. ISO / IEC. (2018). Tecnología de la información - Gestión de servicios - Parte 7: Orientación sobre la integración y correlación de ISO / IEC 20000-1: 2018 a ISO 9001:2015 e ISO / IEC 27001: 2013. Suiza: ISO.
10. ISO/IEC 27000. (2014). Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Descripción general y vocabulario. Vernier, Geneva, Switzerland: ISO.
11. ISO/IEC 27001. (2013). Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. Capital Federal, Argentina: Subcomité de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad (IRAM).
12. IT-Insecurity. (23 de agosto de 2009). *Cultura de Seguridad de la Información: Entendiendo una percepción*. IT-Insecurity: https://insecurityit.blogspot.com/2009/08/cultura-de-seguridad-de-la-informacion.html
13. Laudon, K. C. (2016). Sistemas de Información Gerencial (14º ed.). Pearson.
14. Organización Internacional de Normalización. (s.f.). *Norma ISO 27001*. https://normaiso27001.es/mejora-en-iso-27001/
15. Wikipedia. (s.f). *Ciclo de Deming*. https://es.wikipedia.org/wiki/Ciclo_de_Deming