SGSI en las sociedades de información crediticia

CÁRDENAS, Federico, SOLARES-SOTO, Pedro F.

F. Cárdenas y P. Solares

Universidad Iberoamericana

P. Solares (eds.) Ciencias de los Sistemas de Información y Seguridad. Handbook T-I. -©ECORFAN, Ciudad de México, 2016.

Abstract

The implementation of an Information Security Management System is very useful for organizations of all kinds, however, it is indispensable for those whose operation relies on the safeguarding of sensitive and confidential information. For this, it is convenient to follow a methodology that describes the implementation process adhering to the ISO / IEC 27001 standard and above all, that exists a commitment on the part of the management in order to maintain a process of continuous improvement to the system.

This work intends to take as an example the implantation of an ISMS in an organization such as a Credit Information Society whose characteristics conform to the previously described requirements.

7 Introducción

Los riesgos a los que se enfrentan cada día las organizaciones para conservar la integridad y valor de sus activos requiere que tomen medidas importantes con el propósito de contar con esquemas de seguridad lo suficientemente confiables para que personas internas o externas a la organización vulneren su información. La implantación de un Sistema de Gestión para la Seguridad de la Información se vuelve más crítico conforme aumenta el impacto de una vulnerabilidad a los datos manipulados y resguardados por la empresa.

A continuación, se describirá un modelo de implantación de un SGSI, exponiendo los pasos requeridos a través de un hilo conductor que permita exponer la secuencia derivada de todo sistema basado en un esquema PHVA.

Seguridad de la información

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Indica que esto se logra implantando un conjunto adecuado de controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de software y de hardware. Ya en 1992, el Consejo de la Organización para la Cooperación y el Desarrollo Económico (OCDE), emitió una recomendación relacionada a las directrices de seguridad que deberían adoptar las organizaciones respecto a sus sistemas de información: La seguridad de los sistemas de información tiene por objetivo proteger los intereses de los que cuentan con sistemas de información contra los perjuicios imputables a defectos de disponibilidad, de confidencialidad y de integridad.

La norma ISO/IEC 27001:2013 establece las siguientes definiciones al respecto:

- Confidencialidad: la propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados.

- Integridad: la propiedad de salvaguardar la exactitud y completitud de los activos.

- Disponibilidad: la propiedad de ser accesible y utilizable por una entidad autorizada.

Adicionalmente, la norma ISO/IEC 27002:2009 sugiere que la seguridad en la información debe tomar en consideración la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

Sistemas de Gestión de la Seguridad en la Información

Un Sistema de Gestión de la Seguridad en la Información (SGSI) proporciona un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la protección a activos de información para lograr los objetivos de negocio conforme a una revisión del riesgo y la aceptación a los niveles de riesgo de la organización diseñados para el tratamiento y gestión de riesgos. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

El propósito de un sistema de gestión de la seguridad de la información no es garantizar que la organización contará con una protección total a las distintas amenazas ni reducir a cero sus vulnerabilidades, sino garantizar que los riesgos relacionados a la seguridad de la información sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

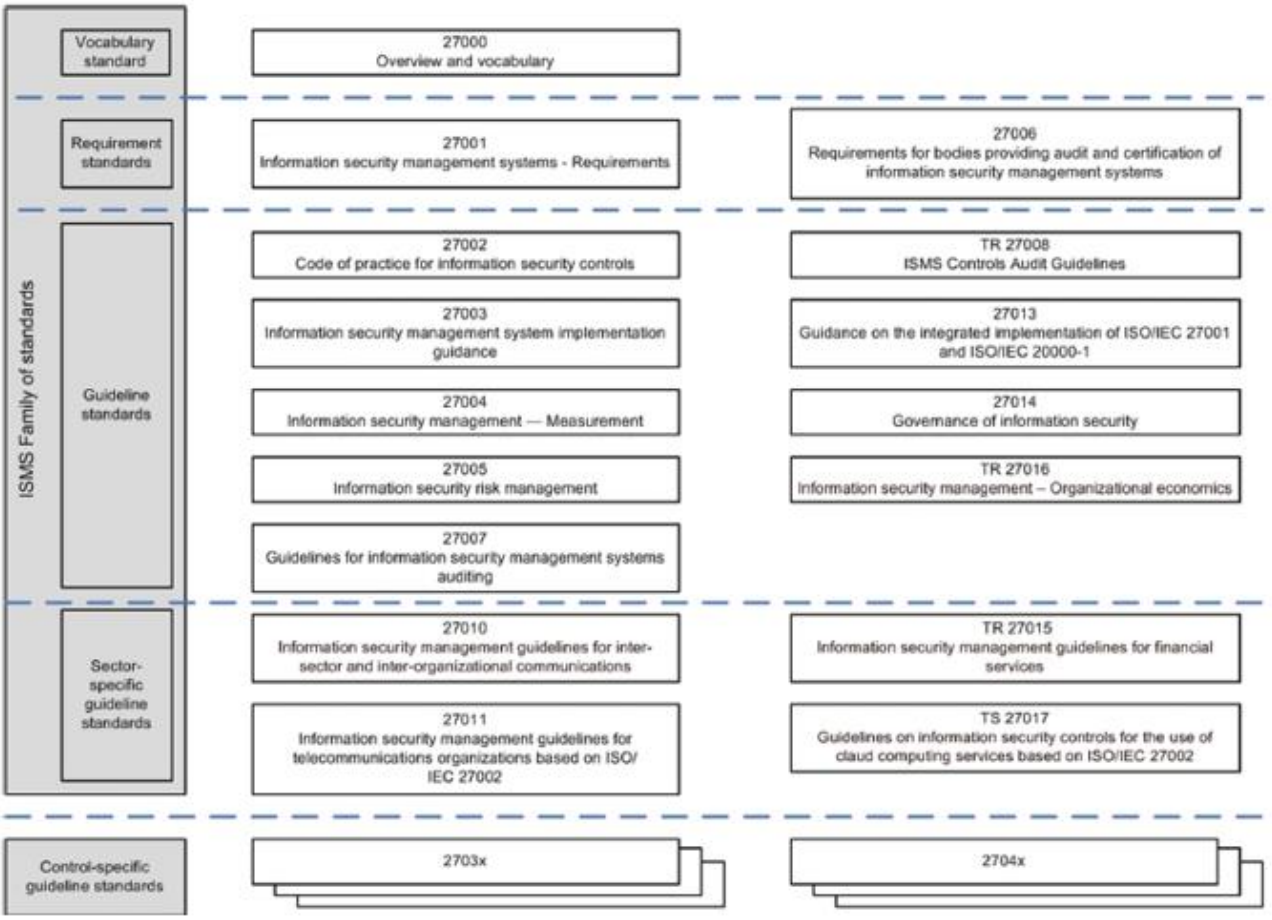
Familia ISO/IEC 27000 y norma ISO/IEC 27001:2013

La familia de normas ISO 27000 corresponden a estándares de seguridad publicadas por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). Dicha serie ayuda a las organizaciones a mantener seguros sus activos de información, tales como información financiera, propiedad intelectual, detalles de sus empleados o información de terceras personas bajo resguardo. ISO/IEC 27001 es el estándar en la familiar que proporciona los requerimientos que debe cubrir un sistema de gestión de seguridad de la información (SGSI). A continuación, se describen las normas que conforman esta familia:

- ISO/IEC 27000, Information security management systems — Overview and vocabulary
- ISO/IEC 27001, Information security management systems — Requirements
- ISO/IEC 27002, Code of practice for information security controls
- ISO/IEC 27003, Information security management system implementation guidance
- ISO/IEC 27004, Information security management — Measurement
- ISO/IEC 27005, Information security risk management
- ISO/IEC 27006, Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007, Guidelines for information security management systems auditing
- ISO/IEC TR 27008, Guidelines for auditors on information security controls
- ISO/IEC 27009, Sector-specific application of ISO/IEC 27001 — Requirements
- ISO/IEC 27010, Information security management for inter-sector and inter-organizational communications

- ISO/IEC 27011, Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27013, Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- ISO/IEC 27014, Governance of information security
- ISO/IEC TR 27015, Information security management guidelines for financial services
- ISO/IEC TR 27016, Information security management — Organizational economics
- ISO/IEC 27017, Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018, Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27019, Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

Figura 7 Familia de estándares para el Sistema de Gestión de la Seguridad en la Información



Para el caso del modelo planteado por ISO/IEC 27001:2013, el sistema de gestión corresponde al PHVA/PDCA (Planear, Hacer, Verificar, Actuar). A continuación, se hace una asociación entre los puntos de la norma y su correspondiente función dentro del PHVA:

Tabla 7 Relación PHVA y puntos de la norma

PHVA	Requisito General	Punto de la norma
PHVA	La organización	Todos, especialmente en el 5 por la responsabilidad de la dirección
P	Crear	4.2.1, el detalle de las actividades de creación está en la definición del alcance, política y análisis de riesgos que figuran más adelante
H	Implementar y operar	4.2.2
V	Supervisar y crear	4.2.3 y 6 y 7
A	antener y mejorar	4.2.4 y 8
PHVA	SAGSI documentado	4.3
P	Actividades empresariales	4.2.1.a y 4.2.1.b
P	Riesgos que esta afronta	4.2.1.c-j

Implementación de un Sistema de Gestión de Seguridad de la Información

Como propone Gomez5, un proyecto para la implantación de un SGSI puede desarrollarse en base a una serie de fases, que se incluyen en la figura 2 y que se describen a continuación.

Lanzamiento y análisis del contexto de la organización. Se deben conocer las circunstancias de la organización, su funcionamiento, las implicaciones, dependencias y requisitos internos y externos y las motivaciones para la implantación de un SGSI.

Definición del alcance. Se determina que elementos formarán parte del SGSI, generalmente identificando procesos de negocio sobre los que se aplicará el sistema.

Definición de los objetivos y la política de seguridad. Además de fijar un marco organizativo, determinando funciones y responsabilidades para la gestión de la seguridad de la información, debe cubrir de manera general todos los aspectos de la seguridad: seguridad física, seguridad lógica, seguridad del personal, y adecuarse a las necesidades y recursos de la organización.

Evaluar los riesgos de la organización. Uno de los métodos para la realización de la evaluación de riesgos es el tradicionalmente seguido de identificar activos, amenazas y vulnerabilidades, de acuerdo a lo siguiente:

- Desarrollar el inventario de activos de información. Se deben identificar los activos que dan soporte a los procesos de negocio en el alcance del SGSI y cuantificar su valor en términos de confidencialidad, integridad y disponibilidad.

- Identificar y valorar amenazas. Se deben identificar todas aquellas amenazas que, en función de la naturaleza del activo, podrían afectarle y asignarles un valor de probabilidad de ocurrencia y de degradación del activo en caso de materialización de la misma, para cada una de las dimensiones.

- Calcular el impacto. Para cada activo y para cada una de las dimensiones de seguridad, se calcula el impacto de la materialización de las amenazas identificadas. Este impacto será una función del valor del activo y de la degradación que produce la amenaza.

- Calcular el riesgo. Para cada activo se calcula el riesgo, que será una función del impacto, calculado en el punto anterior, y de la probabilidad de ocurrencia de la amenaza.

- Identificar a los propietarios de los riesgos. Para los riesgos identificados se debe determinar a la persona o personas responsables de tomar la decisión de la opción de tratamiento de riesgo y de aprobar los planes para la mitigación de los mismos.

- Tratamiento de los riesgos. En este punto se determinan las estrategias a aplicar sobre los riesgos identificados.

- Determinar las medidas de seguridad a implementar. Para gestionar los riesgos será necesario establecer una serie de controles organizativos y técnicos que permitan reducirlos a un nivel aceptable. En el proceso de selección de controles, deben considerarse los beneficios que aportarán y el coste de implantación y mantenimiento de los mismos.

- Evaluar los riesgos residuales. Tras la selección de los controles que permitirán a la organización reducir los riesgos a un nivel aceptable, se deberá calcular cuál será el riesgo que quede tras su implantación, ya que este nunca será cero. El propietario del riesgo tiene que conocer que este riesgo existe y aceptarlo.

- Plan de tratamiento de riesgos. Detallará las actividades necesarias para la implantación de las medidas seleccionadas, incluyendo información sobre plazos, recursos, responsables, etc.

- Elaborar la información documentada necesaria para implementar las medidas seleccionadas. Los procedimientos son la manera de plasmar la implementación de los controles de seguridad y las tareas de administración del SGSI. Un procedimiento debe reflejar fielmente los pasos a seguir para la realización de las tareas, pero debe ser conciso y claro para que no se cometan errores.

- Implementación de los controles y los procedimientos. De una manera planificada y organizada se irán implantando los controles y procesos definidos. Puede ser conveniente comenzar la implantación por aquellas acciones que con un menor esfuerzo aporten un gran valor a la organización (conocidos como Quick Wins).

- Formar y concienciar al personal. Para que la implantación de los procedimientos sea efectiva, es necesario concienciar y formar a todas las personas implicadas. La formación y capacitación de cada usuario deberá ser acorde con las funciones que desempeñe.

- Realizar la auditoría interna y la revisión del SGSI por la dirección. Esto permitirá comprobar el grado de ajuste el SGSI a los requisitos de la norma y determinar si está alineado con los objetivos de la organización.

Figura 7.1 Fases del proyecto de implementación de un SGSI

Para poder implantar un Sistema de Gestión de Seguridad de la Información en una institución, es fundamental tener un conocimiento amplio de la misma, incluyendo sus objetivos de negocio, así como los diferentes actores que giran en torno a ella y que puedan influir en sus fortalezas y debilidades. Esto es importante ya que como se ha mencionado, uno de los propósitos de un SGSI es coadyuvar a que las organizaciones cumplan con los objetivos que se han planteado.

Contexto de la organización. Las Sociedades de Información Crediticia

A continuación, se describe de forma breve la naturaleza de las Sociedades de Información Crediticia.

Los Burós de Crédito son instituciones financieras, autorizadas por la SHCP, previa opinión del Banco de México y de la CNBV. Oficialmente, este tipo de entidades es conocida como Sociedades de Información Crediticia (en adelante, SIC), y son organizaciones que proporcionan servicios de recopilación, manejo y entrega o envío de información relativa al historial crediticio de personas físicas y morales.

Su objetivo es contribuir al desarrollo económico del país ofreciendo servicios que promueven minimizar el riesgo crediticio, al proporcionar información que ayuda a conocer la experiencia de pago de empresas y personas físicas, lo que a su vez, contribuye a formar la cultura del crédito entre la población, al tiempo de promover un sano consumo interno.

En 1996 surge la primera Sociedad de Información Crediticia en México autorizada por la SHCP, con el fin de proporcionar información del comportamiento crediticio de personas físicas. Tiene como socios a la Banca Comercial, a Trans Union Co. (buró crediticio con experiencia en manejo de registros de crédito) y Fair Isaac Co. (empresa con experiencia en modelos de análisis de riesgo).

En 1998 se incorpora el Buró de Personas Morales, con el fin de proporcionar información sobre el comportamiento crediticio de personas morales, y físicas con actividad empresarial. Tiene como socios a la banca comercial, a Trans Union Co. y a Dun & Bradstreet Co., con experiencia a nivel mundial en la evaluación de empresas. En 2005 surge la tercera Sociedad de Información Crediticia en el país contando como socios a Banco Afirme, Coppel, Grupo Chedraui, dos inversionistas privados y Grupo Elektra.

La información que tienen las Sociedades de Información Crediticia reduce los siguientes problemas en la asignación de los créditos:

1. Información asimétrica entre prestamistas y prestatarios, debido a que al haber información crediticia los prestamistas pueden conocer la calidad crediticia de los deudores;

2. Selección adversa, debido a que al haber mayor información se evita el que se considere un posible deudor, de alto riesgo, como de bajo riesgo;

3. Riesgo moral, debido a que se generan incentivos a los acreditados para ser puntuales en su pago, al saber que cualquier incumplimiento afectará su historial crediticio y la posibilidad de obtener créditos en el futuro, y

4. Racionamiento de crédito, debido a que al haber información se evita el que los prestamistas limiten la oferta del crédito a los que demandan créditos, quienes están dispuestos a pagarlo a la tasa de interés a la que se ofrece el crédito.

Las SICs cumplen con los siguientes objetivos:

1. Permite una evaluación completa del desempeño crediticio de los deudores;

2. Facilita el acceso al crédito de los deudores cumplidos con buen historial crediticio;

3. Incrementan la competencia entre instituciones financieras y no financieras que otorgan créditos, al tener acceso a la misma información de las personas;

4. Al haber mayor información sobre la calidad crediticia, permite a las personas con buen historial crediticio el obtener créditos a tasas más bajas;

5. Se reduce la cartera vencida debido a los incentivos que se generan entre los deudores para evitar un mal historial crediticio;

6. Incrementa la movilidad de los clientes debido a que un buen historial crediticio facilita el que se establezca una nueva relación con una institución de crédito;

7. Evita el sobreendeudamiento de los clientes al poder analizarse la capacidad de pago de los clientes, y

8. Se incrementa la posibilidad de que la gente con menores recursos obtenga créditos.

Marco Legal

En julio de 1993 se publicaron enmiendas a la Ley Para la Regulación de Grupos Financieros en el Diario Oficial de la Federación. Entre ellas, la reforma del artículo 33, y la adición de los artículos 33-A y 33-B, con el objeto de crear un nuevo tipo de entidad llamada "sociedad de información crediticia" (buró de crédito). El propósito de dichas reformas fue regular las actividades de reporte de crédito, lo cual hasta ese momento únicamente se había realizado a través del SENICREB del Banco de México.

En enero de 2002, la Ley para Regular las Sociedades de Información Crediticia fue promulgada y se enmendó en 2004, 2008, 2009, 2010 y 2014. Esta ley regula las actividades de los burós de crédito privados. Las provisiones de esta ley son suplementadas por las Reglas Generales a las que Deberán Sujetarse las Operaciones y Actividades de las Sociedades de Información Crediticia y sus Usuarios emitidas por el Banco de México en 2002.

La ley y las reglas antes mencionadas buscan mejorar la veracidad y consecuente credibilidad de los registros de crédito al fortalecer sus normas operacionales. Algunos de los elementos más importantes de dichas regulaciones incluyen mecanismos para proteger los derechos del consumidor. Dichas provisiones establecen requerimientos de consentimiento para la distribución de los reportes de crédito, el derecho de los individuos y empresas a tener acceso a su reporte de crédito completo en los burós de crédito, y procedimientos rápidos y de bajo costo para disputar y corregir la información errónea.

Otras leyes federales que apoyan a los sujetos de los reportes de crédito en sus interacciones con las compañías de reportes de crédito son la Ley de Protección y Defensa al Usuario de Servicios Financieros de 2000, que le provee asistencia al consumidor de enfrentarse a problemas con la misma empresa de reportes de crédito o con un acreedor financiero (bancario o no bancario) y la Ley Federal de Protección al Consumidor de 1992, enmendada en 2004, la cual, entre muchos otros asuntos, es aplicable en casos donde los consumidores experimenten problemas con un acreedor no-financiero.

Marco Regulatorio

Las autoridades que regulan las actividades de las SICs son:

- Secretaría de Hacienda y Crédito Público.

- Banco de México.

- Comisión Nacional Bancaria y de Valores.

- Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros.

Cumplimiento regulatorio referente a seguridad

Existen varias provisiones que exige la Ley para Regular las Sociedades de Información Crediticia requiere como cumplimiento a las SICs en relación a la seguridad de la información:

Artículo 7. Indica que la solicitud para constituirse y operar como Sociedad debe incluir las medidas de seguridad y control a fin de evitar el manejo indebido de la información;

Artículo 19. La Secretaría de Crédito y Crédito Público podrá revocar la autorización otorgada a la Sociedad cuando comenta de manera grave o reiterada violaciones al Secreto Financiero o altere, modifique o elimine reiteradamente algún registro de su base de datos, salvo los supuestos previstos en la ley;

Artículo 22. Exige que la Sociedad adopte las medidas de seguridad y control que resulten necesarias para evitar el manejo indebido de la información, entendiéndose esto último como cualquier acto u omisión que cause daño en su patrimonio al sujeto del que posea información, así como cualquier acción que se traduzca en un beneficio patrimonial a favor de los funcionarios y empleados de la Sociedad o de esta última, siempre y cuando no se derive de la realización propia de su objeto;

Artículo 27. Las Sociedades, al proporcionar información sobre operaciones crediticias y otras de naturaleza análoga, deberán guardar secreto respecto de la identidad de los acreedores, salvo en el supuesto a que se refiere el artículo 39 de la ley, en cuyo caso, informarán directamente a los Clientes el nombre de los acreedores que correspondan;

Artículo 28. Se entenderá que violan las disposiciones relativas al Secreto Financiero tanto la Sociedad, como sus empleados o funcionarios que participen en alguna consulta a sabiendas de que no se ha recabado la autorización correspondiente. Se considerará que los Usuarios, así como sus empleados o funcionarios involucrados, han violado las disposiciones relativas al Secreto Financiero, cuando realicen consultas o divulguen información en contravención a lo establecido en los artículos mencionados en la ley. Las Sociedades, sus empleados y funcionarios tendrán prohibido proporcionar información relativa a datos personales de los Clientes para comercialización de productos o servicios que pretendan ofrecer los Usuarios o cualquier tercero, salvo para la realización de consultas relativas al historial crediticio. Quien proporcione información en contravención a lo establecido en este párrafo, incurrirá en el delito de revelación de secretos a que se refiere el artículo 210 del Código Penal Federal.

Artículo 33. La Sociedad deberá contar con sistemas y procesos para verificar la identidad del Usuario o del Cliente mediante el proceso de autenticación que ésta determine, el cual deberá ser aprobado previamente por el consejo de administración de la Sociedad, a fin de salvaguardar la confidencialidad de la información en los términos de las disposiciones legales aplicables,

Artículo 37. Las Sociedades deberán presentar a la Comisión manuales que establezcan las medidas mínimas de seguridad, mismas que incluirán el transporte de la información, así como la seguridad física, logística y en las comunicaciones. Dichos manuales deberán contener, en su caso, las medidas necesarias para la seguridad del procesamiento externo de datos;

Artículo 38. Los Usuarios de los servicios proporcionados por la Sociedades y cualquier otra persona distinta del Cliente que tenga acceso a sus Reportes de Crédito o Reportes de Crédito Especiales, así como funcionarios, empleados y prestadores de servicios de dichos Usuarios y personas, deberán guardar confidencialidad sobre la información contenida en los referidos reportes y no utilizarla en forma diferente a la autorizada.

Artículo 51. Las Sociedades responderán por los daños que causen a los Clientes al proporcionar información cuando exista culpa grave, dolo o mala fe en el manejo de la base de datos;

En relación a las multas que la CHCP podrá aplicar por incumplimiento, se indica lo siguiente:

- Artículo 60. Sanción con multa de 300 a 5,000 veces el salario mínimo general diario vigente en la CDMX, cuando
- La Sociedad, sus empleados o funcionarios proporcionen a los Usuarios información que incluya la identidad de los acreedores, en contravención a lo previsto por el artículo 27;
- La Sociedad no cuente con los sistemas y procesos previstos en el artículo 33, o no hayan sido aprobados por su consejo de administración;
- Artículo 62. La Comisión sancionará con multa de 2,000 a 20,000 veces el salario mínimo generar diario vigente en la CDMX cuando:
- La Sociedad o Entidad Financiera haga uso o manejo indebido de la información en términos del artículo 22;
- La Sociedad, la Entidad Financiera, o sus funcionarios, empleados o prestadores de servicios incurran en violación al Secreto Financiero o en el delito de revelación de secretos en cualquier forma de las previstas en los artículos 28 y 38;
- Artículo 66. El Banco de México sancionará con multa de 1,000 a 15,000 veces el salario mínimo general vigente en la CDMX, a las Sociedades cuando:
- Omitan sujetarse a lo que el Banco de México les señale en relación con el manejo y control de su base de datos, cuando se acuerde su disolución y liquidación

Alcance del Sistema

Otro aspecto fundamental dentro del proceso de implementación de un SGSI es la identificación de su alcance y límites. Para ello es necesario conocer los procesos que manejan información que deberá ser gestionada en términos de seguridad. En caso de que la organización cuente con el estándar ISO/IEC 90000, se puede tomar el manual de calidad como referencia para la identificación de tales procesos. Una vez realizado esto, es necesario hacer un inventario de activos su origen y destino, así como su clasificación y la tecnología que los soporta.

El inventario de activos debe recoger la siguiente información:

- El nombre del activo, por ejemplo: equipo de usuario, router 014, proyecto, expediente, etc.
- La descripción del activo.
- Categoría a la que pertenece, por ejemplo: equipo, aplicación, servicio, etc.
- Ubicación: el lugar físico en el que se encuentra dentro de la organización.
- Propietario: entendiendo por tal al responsable del activo.

Identificados los activos de información se les debe valorar de acuerdo a su importancia para la empresa. Esta apreciación será lo más objetiva posible, ya que con ella se determinará sobre qué activos se realizará el análisis de riesgos. Por supuesto, se puede hacer una estimación de todos los activos, pero si son muchos, los recursos limitados, o ambas cosas, lo razonable es elegir un grupo de activos reducido para que el análisis de riesgos no sea inabarcable. Por ejemplo, se puede escoger analizar los activos que están por encima de un valor. Para valorar los activos se considerarán los parámetros de confidencialidad, disponibilidad e integridad de los activos, determinándose la importancia que tienen para la organización en una escala de valores predefinida7.

La delimitación del alcance del SGSI es una actividad fundamental, ya que marca la pauta para el resto de las actividades y podrá implicar cambios respecto a la forma en la cual se viene manejando la información dentro de la institución. Más aún, resulta imprescindible que estos cambios se mantengan y mejoren a lo largo del tiempo como parte del proceso de mejora continua del sistema de gestión. Un aspecto importante a considerar es que la norma no requiere aplicarse a toda la organización completa, sino a las partes que más beneficios presenten en relación a los recursos que serán destinados para la implantación del sistema.

Política de Seguridad

Las Políticas de Gestión de la Seguridad de la Información están constituidas por el conjunto de normas reguladoras, procedimientos, reglas y buenas prácticas que determinan el modo en que todos los activos y recursos, incluyendo la información, son gestionados, protegidos y distribuidos dentro de una organización6. Gómez7 menciona que la política de seguridad recogerá las líneas generales de actuación de la organización en una declaración que estará firmada por la dirección, en la que se compromete a velar por la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los activos de información. Además, como parte de este documento o en otro distinto, se debe documentar:

El alcance del sistema, es decir, qué partes de la organización van a estar protegidas por el SGSI. Puede ser la organización entera o una parte relevante de la misma: departamento, servicio o proceso. La recomendación a la hora de decidir el alcance es escoger uno que sea realmente abordable por la empresa. Si es demasiado amplio y no se cuenta con los recursos necesarios para llevar a cabo un SGSI de esa dimensión, el proyecto se alargará y llegará un momento en que se parará, puesto que no hay personal o presupuesto para continuar con él, con la consiguiente frustración de los implicados y la pérdida de tiempo y dinero de la organización.

La estructura de la empresa, un organigrama de las distintas áreas y responsables de la organización, y sus relaciones internas.

Las diferentes responsabilidades de cada parte de la organización: el responsable de seguridad, la dirección, el responsable de sistemas, el personal, etc.

La topología de la red, de manera que se muestren los principales sistemas de información y comunicación que se emplean.

La clasificación de la información, utilizando la nomenclatura de la organización y explicando los criterios de clasificación.

El enfoque y la metodología del análisis de riesgos. Así cualquiera puede verificar los resultados del análisis, ajustándose al razonamiento que se ha seguido para llevarlo a cabo.

Las normas generales de uso de los activos. Estas normas deben existir para evitar incidentes no deseados y utilizaciones indebidas de los activos. Serán hechas públicas, e incluso pueden ser objeto de una entrega formal a los empleados o terceras partes implicadas, de modo que se hagan responsables de las infracciones. Es fundamental establecer unas pautas mínimas en temas como el empleo de las contraseñas y el de las comunicaciones, fuente de numerosas incidencias. Estas normas de uso son un elemento importante en la concienciación del personal, ya que establecen unas pautas de comportamiento, que aunque sean de sentido común y no marquen límites demasiado estrictos, sí indican que la empresa se preocupa al respecto y que los empleados deberían hacer lo mismo.

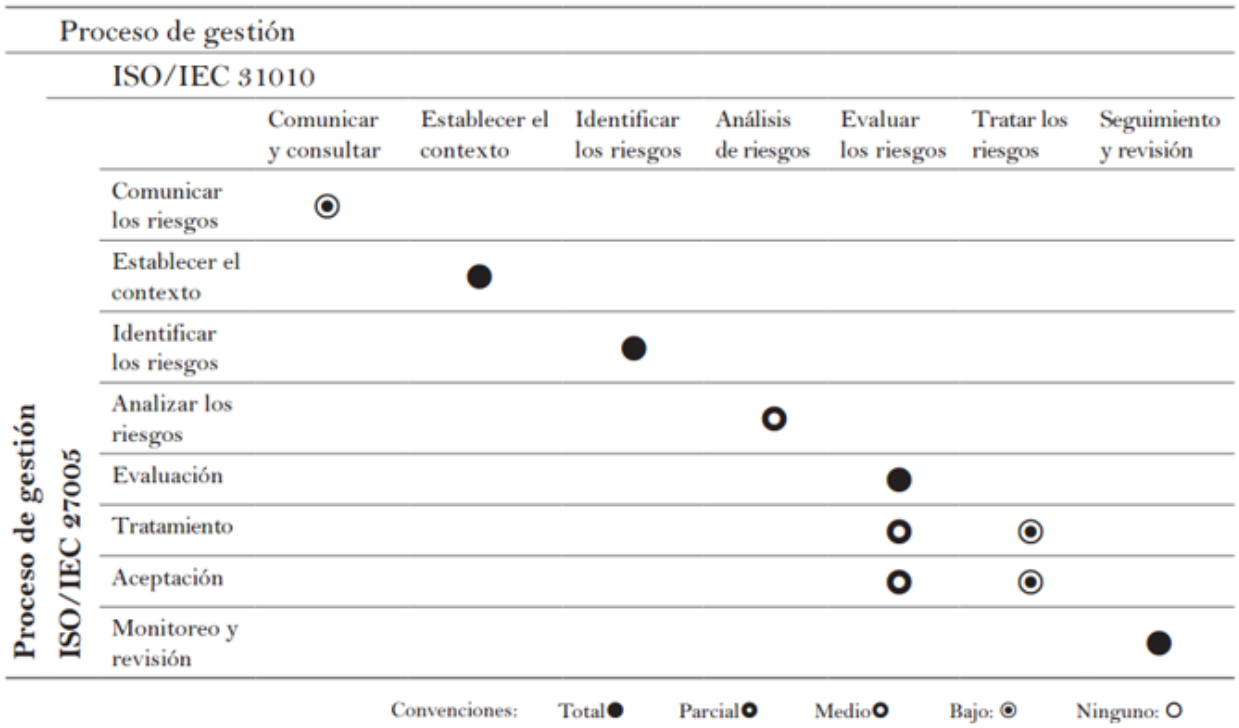
Los objetivos de seguridad que se pretenden alcanzar. Puede ser difícil establecer unos objetivos claros y útiles sin tener datos de partida, pero al menos se deberá intentar expresar qué nivel de seguridad se desea alcanzar. Se puede comenzar por estimar qué metas se quieren lograr en términos de confidencialidad, disponibilidad e integridad. Por ejemplo, para verificar las mejoras en confidencialidad puede utilizarse como métrica el número de incidencias relativas a la confidencialidad, y decidir que el objetivo para este año va a ser tener tres o menos incidencias de este tipo. Con los resultados que se vayan obteniendo, se irá revisando dicho objetivo para ajustarlo a la realidad. Si sistemáticamente obtenemos un valor mucho más elevado, puede que el objetivo no sea realista y haya que revisarlo a la baja.

Gestión del riesgo

Dentro de la familia de normas ISO/IEC 27000 revisada anteriormente se encuentra la norma ISO/IEC 27005, la cual es el estándar internacional que proporciona directrices para la gestión de riesgos de seguridad de la información. Es compatible con los conceptos generales especificados en la norma ISO/ IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de elementos que permitan garantizar la seguridad de la información basada en un enfoque de gestión de riesgos. Es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que podrían comprometer la seguridad de su información8.

Esta norma tiene aspectos comunes con la norma ISO/IEC 31000, Gestión de riesgos – Principios y guías, así como la ISO/IEC 31010 Gestión de riesgos – Técnicas de evaluación de riesgos. Como muestra el estudio de Medina (2015), la diferencia básica entre ambas normas, es que la ISO/IEC 31000 se enfoca en la Gestión de riesgos de manera integral y genérica, mientras que la ISO/IEC 27005 lo hace de forma específica en la Gestión de Riesgos en la Seguridad de la Información. Sin embargo, existe similitud en muchos de los procesos y en la terminología utilizada al definir sus conceptos10.

Figura 7.2 Relación entre los modelos y normas de gestión de riesgos ISO/IEC 27005 e ISO/IEC 31010



Con el propósito de gestionar los riesgos de la organización, se propone emplear la metodología sugerida por Devia, G. A. V., & Pardo (2015), resultante de contrastar los diferentes modelos de riesgos de TI existentes:

Identificar el contexto de la organización. Proporcionando los parámetros básicos para la gestión de riesgo teniendo en cuenta el alcance y los criterios que se van a utilizar durante el proceso. Incluye la consideración de parámetros internos y externos relevantes para la organización, en su conjunto, así como los antecedentes de los riesgos particulares que se están evaluando. Al establecer el contexto, se determinan: el programa de evaluación de los riesgos, los objetivos de la evaluación de riesgos y los criterios del riesgo.

Definir los roles y las responsabilidades del personal relacionado con TI. Determinar los actores que intervienen, llevando un manual de funciones que permita tener claro el papel de cada uno en la organización, de manera que cuando ocurra un riesgo se puedan determinar las posibles fallas por donde se originó el riesgo.

Identificar los activos tecnológicos de la organización. Un activo es algo que tiene valor o utilidad para la organización teniendo en cuenta la continuidad de sus operaciones comerciales; es por eso que un activo necesita protección, para garantizar las operaciones comerciales y la continuidad del negocio.

Identificar los riesgos, amenazas y vulnerabilidades. Los riesgos deben ser identificados de manera que se puedan entender antes de ser analizados y gestionados correctamente. Esta identificación debe tener un enfoque detallado que permita abarcar todos los eventos posibles, de modo que se clasifiquen los riesgos en las categorías definidas en la estrategia de gestión del riesgo, de tal manera que los riesgos formen una línea base para el inicio de actividades en la gestión de riesgo.

Los riesgos deben ser revisados periódicamente para reexaminar las posibles fuentes de riesgo y revisar las condiciones cambiantes, revisando los riesgos que se pasaron por alto o aquellos que no existían en la última revisión.

Analizar los riesgos. El análisis de riesgos implica su identificación a partir de fuentes internas y externas; cada riesgo es evaluado para determinar su probabilidad y sus consecuencias. Los riesgos se categorizan con base en la evaluación establecida en la estrategia de gestión de riesgos, proporcionando información suficiente para su manejo, estableciendo un nivel de análisis con base en lo que es apropiado y razonable.

Evaluar los riesgos, determinando el nivel de riesgo. Este es el proceso donde se consolida la identificación, el análisis y la evaluación de los riesgos, es en este punto donde se determina su prioridad para el tratamiento adecuado.

Tratar los riesgos, definir e implementar los planes de mitigación. Terminada la evaluación del riesgo, se ejecutan las medidas correctivas, se escoge una serie de opciones para mitigar el riesgo; este es un proceso repetitivo que tiene como fin determinar su tolerabilidad en contra de los criterios establecidos, con el fin de decidir si se requiere un tratamiento posterior. Los riesgos son monitoreados cuando superan los umbrales establecidos, los planes de mitigación de riesgos se despliegan para devolver el esfuerzo afectado a un nivel de riesgo aceptable. Si el riesgo no puede ser mitigado, se puede invocar un plan de contingencia.

Aceptar el riesgo. En este punto del proceso, toma parte la alta dirección de la organización que es la encargada de determinar el nivel de impacto del riesgo y de decidir si se acepta o no, teniendo en cuenta sus consecuencias. Aceptar el riesgo incluye asumir las responsabilidades frente a las insuficiencias encontradas luego de haber tratado el riesgo (si ha quedado algún riesgo residual).

Llevar un control de seguimiento y monitoreo del riesgo tratado. Como parte del proceso de gestión, los riesgos y los controles deben ser monitoreados y revisados periódicamente para verificar que las hipótesis sobre los riesgos sigan siendo válidas.

Registrar el proceso de gestión de riesgos. Se debe llevar un histórico de todos los incidentes, que permita llevar una auditoría independiente en la gestión de riesgos con el fin de garantizar que se ha realizado una buena gerencia de riesgos8.

Información documentada sobre procesos

Como parte de la implantación del SGSI, es necesario documentar la forma en la cual operará el sistema. Para ello se deberá recurrir a las políticas, normas, procedimientos e instrucciones técnicas que soporten el modelo.

Implementación del SGSI

Para poner en marcha el SGSI la dirección tiene que aprobar la documentación desarrollada en las actividades detalladas en el punto anterior y proveer los recursos necesarios para ejecutar las actividades. Para ello es necesario contar con el plan de tratamiento del riesgo el cual deberá incluir los controles necesarios para atender los riesgos conforme a la tolerancia aprobada por la dirección.

Supervisión y verificación del sistema

Como parte de la implementación del sistema, es necesario contar con un mecanismo que permita verificar que el plan de tratamiento a los riesgos cumple su cometido, así como validar que los objetivos de seguridad se han cumplido de manera eficaz y que las incidencias están siendo atendidas conforme los procedimientos previstos. Para llevar a cabo esta fase se realizan una serie de acciones: las revisiones periódicas, las auditorías internas y la revisión del sistema por la dirección5.

Revisiones periódicas

La organización requiere contar con un conjunto de revisiones que permitan verificar que el sistema cumple con sus objetivos definidos y documentarlos correctamente. Lo anterior permitirá validar el progreso de las actividades programadas que se emplearán para el cumplimento de los objetos.

Auditoría interna

El propósito de las auditorías internas es poder detectar y documentar de forma veraz e imparcial las vulnerabilidades que presenta una organización que cuenta con el SGSI, a fin de garantizar que tal sistema está cumpliendo con los requisitos de la norma por medio de sus objetivos de control, controles, procesos y procedimientos existentes.

La documentación que deberá revisarse dentro de las auditorías internas es la siguiente:

- Política, objetivos y alcance.
- Procedimientos y mecanismos de control de soporte.
- Metodología de evaluación de riesgos.
- Informe de evaluación de riesgos.
- Plan de tratamiento de riesgos.
- Procedimientos específicos para la planificación, operación y control de los procesos de seguridad de la información, así como los relacionados con la medición de la eficacia de los controles.
- Otros registros exigidos por la norma ISO 27001.
- Declaración de aplicabilidad de los controles.

Revisión del sistema por la dirección

Otro aspecto importante dentro de la supervisión del sistema es la validación que realiza la dirección a fin de corroborar que las acciones están encaminadas de forma correcta y alineadas de forma adecuada a sus expectativas.

Mejora del sistema

Este punto concreta el ciclo PHVA, al tomar las medidas necesarias a fin de corregir los hallazgos detectados durante la fase de supervisión y validación. De esta forma, el proceso de mejora continua se mantiene durante cada iteración al poner en marcha las acciones preventivas y correctivas necesarias.

7.2 Conclusiones

Para las Sociedades de Información Crediticia es indispensable contar con un sistema de gestión de seguridad de la información que permita identificar y controlar los diferentes riesgos que puedan comprometer la información que resguardan y, por ende, el secreto financiero asociado. Asimismo, se tiene el beneficio adicional de reforzar el sistema de gestión de riesgos que pudiera tener implementada la empresa (tal como ISO/IEC 31000:2009), al contar con una visibilidad más detallada en las amenazas que pudieran comprometer aspectos específicos de seguridad de la organización y robustecer la continuidad y disponibilidad del negocio. De esta forma es posible dar cumplimiento y conformidad a la regulación a la que están sujetas. Como beneficio complementario, permite generar credibilidad y confianza a sus clientes, socios y proveedores al contar con una certificación emitida por un tercero, alineada a las mejores prácticas internacionales.

Para lograr lo anterior, es imprescindible que la empresa cuente con el compromiso de la Alta Dirección, tener un gobierno corporativo maduro y una cadena de responsabilidades claramente definida, así como sensibilizar a la toda la organización respecto a la importancia de la seguridad y la gestión de riesgos a fin de hacerlos partícipes de este esfuerzo de mejora continua que se busca en el sistema.

Como pudo mostrarse en el desarrollo del contexto de la empresa, son varios los aspectos que deben ser atendidos por una Sociedad de Información Crediticia en términos de cumplimiento por la legislación actual, los cuales pueden atender su conformidad por medio de la norma ISO/IEC 27001. Al momento, las SICs existentes en México se encuentran certificadas en el sistema de gestión mencionado y mantienen el ciclo de mejora continua dentro de sus procesos.

7.3 Referencias

Gil Hubert, J. (2004). The Mexican Credit Reporting Industry Reform: A Case Study.

CNBV, "Ley para Regular las Sociedades de Información Crediticia". Enero 2014, Disponible en: http://www.cnbv.gob.mx/Paginas/NORMATIVIDAD.aspx

Mundial, B. (2005). Sistemas de reporte de préstamos bancarios y créditos en México. México: Centro de Estudios Monetarios Latinoamericanos, Banco Mundial y First Initiative.

Gómez Fernández, Luis, and Fernández Rivero, Pedro Pablo. Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad. Madrid, ES: AENOR - Asociación Española de Normalización y Certificación, 2015.

Fernández Sánchez, Carlos Manuel, Piattini Velthuis, Mario. Modelo para el gobierno de las TIC basado en las normas ISO. Madrid, ES: AENOR - Asociación Española de Normalización y Certificación, 2012

Gómez Vieites, Álvaro. Seguridad en equipos informáticos. Madrid, ES: RA-MA Editorial, 2014. ProQuest ebrary. Web. 5 November 2016.

Gómez Fernández, Luis, and Andrés Álvarez, Ana. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. Madrid, ES: AENOR - Asociación Española de Normalización y Certificación, 2012.

Devia, G. A. V., & Pardo, C. J. (2014). Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT. Sistemas & Telemática, 12(30), 35-48.

Castro, A. R., & Bayona, Z. O. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. Ingeniería, 16(2), 56-66.

Medina Tapia, M. A. (2015). Estudio analítico de la compatibilidad e integración de las normas ISO/IEC 31000 e ISO/IEC 27005 referente a riesgos en la seguridad de información (Doctoral dissertation, Universidad de las Fuerzas Armadas ESPE. Carrera de Ingeniería en Sistemas e Informática.).