

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS Y COMPUTACIÓN

TEMA: DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA COMERCIO ELECTRÓNICO BASADO EN LA ISO 27001 PARA PEQUEÑAS Y MEDIANAS EMPRESAS EN LA CIUDAD DE QUITO

AUTOR: ÁNGEL PATRICIO SÁNCHEZ SOLÁ

DIRECTOR: ING. FRANCISCO RODRÍGUEZ

QUITO, NOVIEMBRE DEL 2013

DEDICATORIA

Este trabajo está dedicado principalmente a Dios, porque él ha sido quién me bendice, protege y cuida cada segundo de mi vida.

A mis padres Piedad Solá y Ángel Sánchez; ya que con su esfuerzo y sacrificio diario supieron sacarme adelante, demostrándome su incondicional apoyo y amor. A mi abuelita Genoveva Solá(+) quien desde niño me supo cuidar en base a valores, y ahora desde el cielo recibo sus bendiciones.

A ellos, quienes siempre me guiaron, me aconsejaron y me tendieron sus manos en los momentos difíciles, es esta dedicatoria, como mi principal fuente de inspiración tanto en mi vida profesional como personal.

A mi esposa Paola Zambrano, por ser mi compañera fiel, por su apoyo incondicional y sobre todo por la fortaleza con la que toma mi mano y nuestro hogar.

A mi hijo Matías Sánchez Zambrano, la bendición más grande que me pudo dar Dios, fuente de inspiración diaria y por quién lucharé el resto de mi vida para inculcarle los valores que me enseñaron mis Padres y mi Abuelita.

Ángel Patricio Sánchez Solá

AGRADECIMIENTO

Agradezco a Dios por las infinitas bendiciones, por darme lo más importante que es la vida, y la fortaleza en los momentos más difíciles.

A mis Padres Piedad Solá y Ángel Sánchez, mi abuelita Genoveva Solá por su incondicional amor, cariño y enseñanzas que siempre me brindaron.

A mis hermanas Margarita, Sofía (+) y Jenny por compartir mis alegrías, fracasos y por alentarme día a día a ser mejor.

A mi Director de tesis Ing. Francisco Rodríguez, por su guía e incondicional apoyo en el desarrollo de esta disertación de tesis.

A mis revisores Ing. Suyana Arcos e Ing. Oswaldo Luna, por sus aportes, consejos y experiencias, que me sirvieron para el desarrollo de esta disertación de tesis.

A mis profesores, que a lo largo de esta carrera supieron compartirnos sus valiosos conocimientos.

Ángel Patricio Sánchez Solá

ÍNDICE

1 CAPÍTULO 1: GENERALIDADES 8

1.1 JUSTIFICACIÓN E IMPORTANCIA 8
1.2 PLANTEAMIENTO Y DELIMITACIÓN DEL TEMA 10
1.3 CONTEXTUALIZACIÓN DEL TEMA 11
1.4 OBJETIVOS 12
1.4.1 Objetivo General 12
1.4.2 Objetivos Específicos 12
1.5 METODOLOGÍA Y TÉCNICAS 13

2 CAPÍTULO 1: SEGURIDAD DE LA INFORMACIÓN 15

2.1 DEFINICIÓN 15
2.2 EVOLUCIÓN 16
2.3 IMPORTANCIA 17
2.4 OBJETIVOS 19
2.5 ÁREAS DE PROCESO DE LA SEGURIDAD 21
2.5.1 Riesgos 21
2.5.2 Ingeniería 23
2.5.3 Aseguramiento 24
2.6 ELEMENTOS DE GESTIÓN DE LA SEGURIDAD 26
2.7 DIFERENCIAS CON SEGURIDAD INFORMÁTICA 29

3 CAPÍTULO 2: NORMAS ISO 32

3.1 ISO 32
3.1.1 Definición de la ISO 32
3.1.2 Historia de la ISO 32
3.1.3 Beneficios de las Normas Internacionales ISO 33
3.1.4 Procedimiento para el Desarrollo de las Normas ISO 34
3.2 FAMILIA DE LAS NORMAS ISO 27000 37
3.2.1 Definición de las Normas ISO 27000 37
3.2.2 Origen de las Normas ISO 27000 38
3.2.3 Beneficios de las Normas ISO 27000 40
3.2.4 Serie 27000 42
3.2.5 Contenido de la Serie 27000 44
3.3 NORMA ISO 27001 54
3.3.1 Definición de la ISO 270001 54

3.3.2 Componentes básicos de la ISO 270001 56
3.3.3 Estructura del Modelo de SGSI 57
3.3.4 Fases del SGSI..... 59
3.3.4.1 Fase de Planificación..... 60
3.3.4.2 Fase de Implementación..... 61
3.3.4.3 Fase de Verificación 62
3.3.4.4 Fase de Mantenimiento y mejora 63

4 CAPITULO 3: SISTEMA DE GESTIÓN 64

4.1 PYMES ECUATORIANAS 64
4.1.1 Introducción 64
4.1.2 Procesos..... 66
4.2 GENERALIDADES..... 72
4.3 PROCEDIMIENTO..... 73
4.4 DESARROLLO 77
4.5 PROPUESTA..... 79
4.5.1 Fase de Planificación..... 79
4.5.1.1 Alcance y límite del SGSI..... 79
4.5.1.2 Políticas de Seguridad 79
4.5.1.3 Identificación de Activos y sus riesgos 91
4.5.1.4 Control de Riesgos 97
4.5.1.5 Fijación de controles y objetivos de control 97
4.5.1.6 Definición de la Declaración de la Aplicabilidad..... 107
4.5.2 Fase de Implementación 108
4.5.3 Fase de Verificación 110
4.5.4 Fase de Mantenimiento y mejora..... 111

CONCLUSIONES..... 113

RECOMENDACIONES..... 11317

BIBLIOGRAFÍA..... 11320

ANEXOS…. ……...123

ANEXO 1: MARCO CONCEPTUAL 123
ANEXO 2: ISO/IEC 270001:2005 125

ÍNDICE DE TABLAS

Tabla 4.1 Políticas de Seguridad de Activos. 81
Tabla 4.2 Políticas de Seguridad del Personal. 82
Tabla 4.3 Políticas de Seguridad Física. 83
Tabla 4.4 Políticas de Control de Acceso e Ingreso a los Sistemas. 84
Tabla 4.5 Políticas de Software. 85
Tabla 4.6 Políticas de Redes 86
Tabla 4.7 Políticas de Correo electrónico. 87
Tabla 4.8 Políticas de Comercio electrónico. 88
Tabla 4.9 Políticas de Internet. 89
Tabla 4.10 Políticas de Control de firewall. 90
Tabla 4.11 Políticas de Backups. 91
Tabla 4.12 Formato Activos. 93
Tabla 4.13 Formato Factores de riesgo. 94
Tabla 4.14 Formato Consecuencias y Medidas. 96
Tabla 4.15 Formato Vulnerabilidad. 96
Tabla 4.16 Controles. 106
Tabla 4.17 Implementación del SGSI. 109
Tabla 4.18 Verificación del SGSI. 111
Tabla 4.19 Mantenimiento y mejora del SGSI. 112

ÍNDICE DE ILUSTRACIONES

Ilustración 2.1 Objetivos de la Seguridad de la Informacipon.....19
Ilustración 2.2 Componentes del proceso de riesgos.....22
Ilustración 2.3 Áreas de proceso de la seguridad. 23
Ilustración 2.4 Esquema del Proceso de Aseguramiento de la seguridad. 25
Ilustración 2.5 Elementos del proceso de gestión de la seguridad.....26
Ilustración 2.6 Relación entre los elementos de la Gestión de la Información. 27
Ilustración 2.7 Valor agregado de la implementación de la seguridad de la información. 28
Ilustración 2.8 Campos de Acción de la Seguridad de la Información y de la Informática. 30
Ilustración 3.1 Beneficios de las ISO.....34
Ilustración 3.2 Proceso para el desarrollo de las Normas ISO. 35
Ilustración 3.3 Historia de las Normas ISO 27000.....40
Ilustración 3.4 Beneficios de las Normas ISO 27000. 41
Ilustración 3.5 Beneficio Normas ISO 27000.....42
Ilustración 3.6 Desarrollo de Estándares de la Serie 27000.....43
Ilustración 3.7 Componentes básicos del SGSI. 56
Ilustración 3.8 Modelo SGSI.....59
Ilustración 3.9 Fases del SGSI.....60
Ilustración 4.1. Proceso de Venta. 67
Ilustración 4.2. Proceso de Compra. 68
Ilustración 4.3. Proceso de Producción. 69
Ilustración 4.4 Proceso de eCommerce. 71
Ilustración 4.5 Como garantizar la seguridad de la información. 74
Ilustración 4.6 Procedimiento SGI a seguir. 76
Ilustración 4.7 Pasos para la implementación de un SGSI.....78

1 CAPÍTULO 1: GENERALIDADES

1.1 JUSTIFICACIÓN E IMPORTANCIA

La información es el patrimonio vital de toda organización, en la actualidad ha surgido la aparición de nuevas amenazas en los sistemas informáticos, principalmente en lo referente al hackeo de los mismos, teniendo el riesgo de que la información privada de una organización sea revelada o no sea utilizada apropiadamente.

Esta preocupación debe ser adecuadamente atendida y así, poder mantener la operatividad y rentabilidad de una Organización, es por esto, que el correcto manejo de la información, es trascendental para el éxito de cualquier organización y por ende, para su continuidad en el mercado. Debido a la importancia de este recurso, su aseguramiento debe ser un objetivo primordial en las organizaciones.

Con el fin de suplir dichas necesidades de seguridad, muchas organizaciones han implementado estándares, mejores prácticas, metodologías y/o herramientas que faciliten la gestión eficiente de la seguridad de la información.

Actualmente, se cuenta con estándares internacionales aceptados que proporcionan mecanismos de seguridad probados, con resultados ideales y que deberían ser implementados por todas las organizaciones.

En este sentido, sobresalen las Normas ISO 27001, la cuales proveen los requisitos necesarios para gestionar la Seguridad de la Información, minimizando los riesgos a los que está expuesta, en cualquier organización.

Adicionalmente, es importante considerar que debido a la globalización, las pequeñas y medias organizaciones buscan tener una ventaja con la competencia, para ello la gestión de seguridad de la información toma gran relevancia.

Una correcta gestión de la información, permite a las organizaciones obtener un beneficio básico: la administración efectiva y controlada de la misma. Este beneficio se traduce en mayor eficiencia y eficacia de los procesos, lo que a su vez genera mayor rentabilidad para la empresa dentro un marco de mejora continua.

Es así, que el diseño de un sistema de gestión de la seguridad de la información para comercio electrónico basado en la ISO 27001, aportará gratuita y substancialmente a la adecuada gestión informática en pequeñas y medianas empresas en la ciudad de Quito, las cuales en su mayoría no

manejan un departamento exclusivo de Sistemas o a su vez no poseen los recursos necesarios para una asesoría de este tipo.

Dicho diseño, se basará en los tres principios básicos de la seguridad: confidencialidad, integridad y disponibilidad, centrándose especialmente en la protección frente a posibles hackeos que ésta puede tener.

1.2 PLANTEAMIENTO Y DELIMITACIÓN DEL TEMA

Gran cantidad de información es altamente utilizada, desde los hogares hasta las organizaciones; por esta razón, es importante determinar qué hacer para protegerla, y esto se obtiene con la fijación de políticas de seguridad.

Con este proyecto, se busca proponer políticas que permitan una adecuada gestión de la información de cualquier organización o institución ecuatoriana, acordes a la realidad nacional, en especial frente a la amenaza de posibles hackeos en los sistemas informáticos.

Para el desarrollo del mismo, se utilizarán como guía principal las Normas ISO 27000, específicamente la ISO 27001; ya que, estos estándares

proporcionan las pautas referentes a la gestión de la seguridad, la cual, como se indicó anteriormente, se basará en los tres pilares fundamentales: confidencialidad, integridad y disponibilidad.

1.3 CONTEXTUALIZACIÓN DEL TEMA

Debido a que la seguridad de la información es un componente crítico de la estrategia de negocio en cualquier organización, este proyecto permitirá entender la importancia de definir políticas, procedimientos y estándares de seguridad, para el comercio eléctrico de Pymes basados en recomendaciones a nivel internacional.

En esencia, se busca proponer un sistema de gestión basado en un plan de acción para el mejoramiento de la seguridad de la información en una pequeña o mediana empresa quiteña.

De esto se genera dos cuestionamientos:

- ¿De qué manera la Aplicación de las Normas ISO 27001, afectarán la Gestión de la Seguridad de la Información en una Organización?.

- ¿La Aplicación de las Normas ISO 27001, optimizará la Seguridad de la información en una Pyme, en especial frente a hackeos en sus Sistemas de Comercio electrónico?.

1.4 OBJETIVOS

1.4.1 Objetivo General

Desarrollar un sistema de gestión de la seguridad de la información para comercio electrónico, el cual contenga las principales políticas de seguridad de la información, bajo las Normas ISO 27001, y que sirva como plan de acción para el mejoramiento de la seguridad de la información en una Pyme de la ciudad de Quito, de acuerdo a la realidad de las mismas; a fin de alcanzar la eficiencia y eficacia, en las actividades de resguardo y protección de la información, en especial frente a posibles hackeos.

1.4.2 Objetivos Específicos

- Describir y detallar los conceptos de la seguridad de la información y lo que ésta implica.
- Exponer las Normas ISO 27001 y distinguir la respectiva aplicación de las mismas en una organización de pequeño y mediano tamaño.

- Analizar el entorno y funcionamiento de las Pymes quiteñas, con el fin de exponer políticas de seguridad acorde a la situación de las mismas.
- Establecer los requisitos básicos para la implantación, mantenimiento y mejoramiento de la gestión de procesos de Seguridad de la información en una Pyme ecuatoriana.
- Desarrollar un sistema de gestión de la información para comercio electrónico, que permita fortalecer su seguridad, asegurando la disponibilidad, el acceso, el control, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, frente a posibles hackeos.

1.5 METODOLOGÍA Y TÉCNICAS

Tomando en cuenta las características del proyecto, se propone recurrir a los siguientes métodos:

- **Método inductivo-deductivo**: Se lo utilizará para describir de manera particular los fundamentos teóricos en los cuales se basa la seguridad de la información, así como de las normas a aplicar.
- **Método histórico-lógico**: En el desarrollo de la investigación, se revisarán los antecedentes y los hechos de mayor importancia

sobre la gestión de la seguridad de la información, y de esta manera presentar una propuesta de políticas de seguridad cumpliendo la Normativa señalada; para así ofrecer una solución válida para el mejoramiento de la seguridad de la información en organizaciones o instituciones.

Por otra parte, las fuentes a utilizar son las siguientes:

- **Fuentes Primarias**: Información bibliográfica (publicaciones impresas y digitales).
- **Fuentes Secundarias**: Entrevistas a expertos.

Adicionalmente, es importante, detallar las variables a considerar en el desarrollo del proyecto:

- **Independiente**: Normas ISO 27001.
- **Dependiente**: Sistema de Gestión de la Seguridad de la Información.

2 CAPÍTULO 1: SEGURIDAD DE LA INFORMACIÓN

2.1 DEFINICIÓN

Se entiende por seguridad de la información al “conjunto de sistemas y procedimientos que garantizan: la confidencialidad, la integridad y la disponibilidad de la información. Quizás se eche de menos en ella la falta de autenticación, el no repudio tanto en origen como destino y el sellado de tiempo” (DEL PESO, 2003, p. 56).

La Seguridad de la Información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada (ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD, 2013).

Por lo tanto, la seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. En base a esto, la seguridad puede ser entendida como un estado de cualquier sistema o tipo de información para que esté libre de peligro, daño o riesgo, entendiendo a estos últimos como todo aquello que pueda afectar su funcionamiento directo o a los resultados que se obtienen.

> La seguridad actual de toda organización es, por tanto, un proceso de mejora continua, en la que han de estar implicados todos los departamentos de la empresa, que debe estar bajo un modelo de madurez eficaz que monitorice, con valores cuantitativos y cualitativos, los riesgos de seguridad para poder actuar, no sólo de forma reactiva, sino proactiva y preventiva. Además, tiene que permitir controlar y observar con el máximo grado de detalle y profundidad, todos los aspectos del ciclo de vida infinito de mejora de la seguridad del negocio, haciéndolo acorde con los objetivos de productividad, competitividad y supervivencia, a veces cambiantes (AREITIO, 2008, p.11).

La seguridad en la información abarca a todas las medidas preventivas y reactivas que permite resguardar y proteger la información, cuyo fin es mantener la confidencialidad, disponibilidad e integridad de la misma.

2.2 EVOLUCIÓN

La tendencia, cada vez más dominante, hacia la interconectividad y la interoperabilidad de las redes, de las máquinas de computación, de las aplicaciones, e incluso, de las empresas, ha situado a la seguridad de los sistemas de información como un elemento central en todo desarrollo de la

sociedad. La seguridad ha pasado de utilizarse para preservar los datos clasificados del gobierno en cuestiones militares o diplomáticas, a tener una aplicación de dimensiones inimaginables y crecientes que incluye transacciones financieras, acuerdos contractuales, información personal, archivos médicos, comercio y negocios por Internet, domótica, inteligencia ambiental y computación ubicua. Por ello, se hace imprescindible que las necesidades de seguridad potenciales se tengan en cuenta y se determinen para todo tipo de aplicaciones. Este desplazamiento del enfoque de las cuestiones de seguridad, desde el nivel gubernamental al resto de la sociedad, ha elevado la importancia de la seguridad, y ha pasado a ser una disciplina cada vez más crítica, necesaria, obligatoria y un componente clave en todo título y de proyectos de sistemas de información. (AREITIO, 2008, p. 2).

2.3 IMPORTANCIA

En la actualidad, las empresas se enfrentan con riesgos e inseguridades ocasionados por una amplia variedad de fuentes que pueden dañar de forma importante sus sistemas de información, así como también poner en peligro la continuidad del negocio.

Ante esto es de vital importancia que las empresas evalúen los riesgos asociados, establezcan las estrategias y controles adecuados que aseguren una permanente protección de la información y de sus sistemas.

Es así, que una gestión eficaz de la seguridad de la información permitirá:

- Asegurar el acceso a la información, previniendo la divulgación de la misma a personas o sistemas no autorizados.
- Asegurar la información con métodos de proceso exactos y completos, buscando mantener los datos libres de modificaciones no autorizadas.
- Asegurar que usuarios autorizados tengan acceso a la información y activos asociados cuando lo requieran, es decir que pueden encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

La seguridad puede observarse en diferentes planos de la sociedad, como: una comunidad, una organización, un sistema, un producto, o un servicio. El desarrollo e implantación creciente en los últimos daños de las TIC (Tecnologías de la Información y la Comunicación) en los sistemas de información de todo tipo de organizaciones, ha transformado el modo de actuar y de relación en todos los ámbitos. Este impacto en el mundo empresarial, por ejemplo, a través de Internet, está posibilitando almacenar, procesar o compartir información. En el actual entorno competitivo de la sociedad de la información y del conocimiento, la adecuada gestión de la seguridad de la información es de vital importancia para la supervivencia de una organización (AREITIO, 2008, p. 2).

2.4 OBJETIVOS

Los objetivos principales de la seguridad de la información, se muestran en la siguiente ilustración:

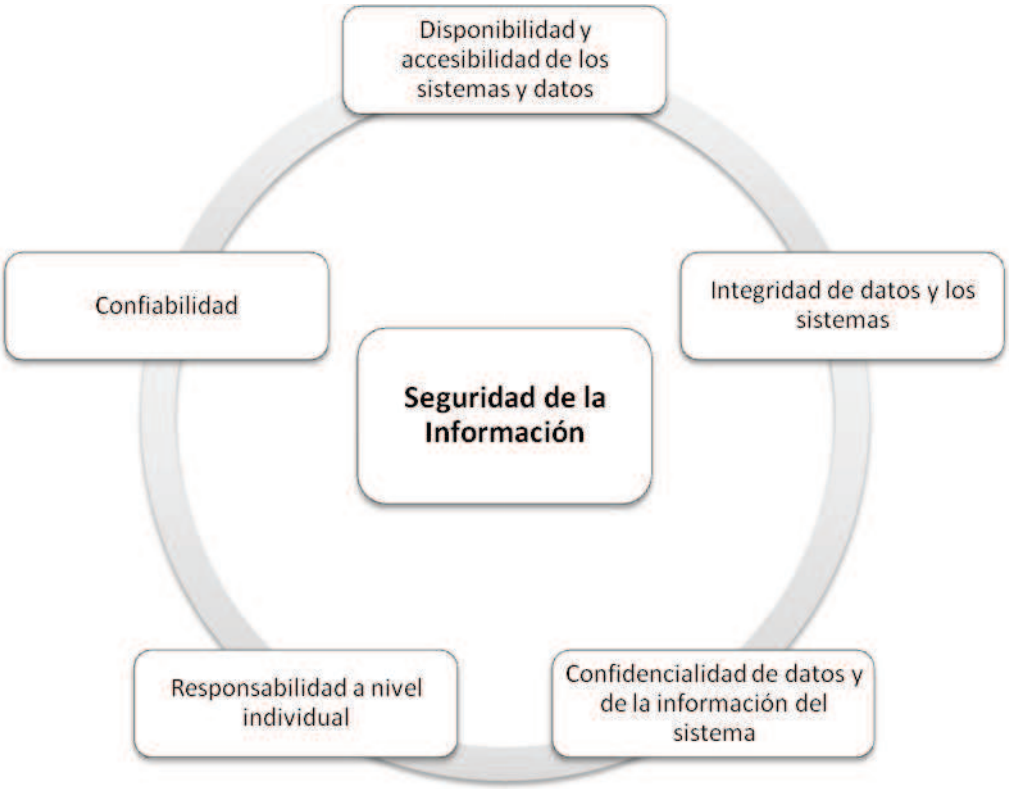


Ilustración 2.1 Objetivos de la Seguridad de la Información.

Fuente: AREITIO (2008, p. 3).

Asimismo, existen otros objetivos más generales de la seguridad, entre los que se pueden identificar los siguientes:

- Conocer todos los riesgos de seguridad asociados a una empresa u organización.
- Establecer un conjunto equilibrado de requisitos de seguridad de acuerdo con los riesgos identificados, para satisfacer las necesidades de un determinado proceso de negocio.
- Transformar las necesidades de seguridad en una guía de seguridad, para integrarla en las actividades de otras disciplinas implicadas en un proyecto y en unos descriptores de configuración u operación de un sistema.
- Establecer la confianza o garantía en la corrección y efectividad de los mecanismos de seguridad.
- Determinar los impactos operacionales relacionados a habilidades de seguridad residuales de un sistema o su operación, es decir, que los riesgos sean aceptables.
- Integrar los esfuerzos de todas las disciplinas de ingeniería y especialidades en un intento combinado de la confianza fidedigna de un sistema (AREITIO, 2008, p.p. 3-4).

En conclusión, la meta de la seguridad de la información es permitir que una organización cumpla con sus objetivos institucionales, implementando sistemas que tengan un especial cuidado y consideración hacia los riesgos relativos a la misma.

2.5 ÁREAS DE PROCESO DE LA SEGURIDAD

Todo modelo de madurez de seguridad divide la seguridad en tres grandes áreas: el proceso de gestión de riesgos, el proceso de ingeniería de seguridad y el proceso de aseguramiento (AREITIO, 2008, p. 7).

Aunque estas áreas no son independientes entre sí, es posible considerarlas por separado. Estas tres áreas operan de forma conjunta, con el fin de asegurar que el proceso de seguridad realice los objetivos anteriormente descritos

2.5.1 Riesgos

En el nivel más simple, el proceso de gestión de riesgos identifica y prioriza los peligros inherentes al desarrollo de un producto, sistema u organización. La gestión del riesgo es una parte importante de la gestión de la seguridad y se define como el proceso que se encarga de identificar y cuantificar la probabilidad de que se produzcan amenazas y de establecer un nivel aceptable de riesgo para la organización, considerando el impacto potencial de un incidente no deseado. La valoración de riesgos es el proceso

consistente en identificar los problemas antes de que aparezcan descritos (AREITIO, 2008, p. 7).

Como se muestra en la figura, los componentes del riesgo son tres: amenaza, vulnerabilidad e impacto.



Ilustración 2.2 Componentes del proceso de riesgos.

Fuente: AREITIO (2008, p. 8).

Los riesgos disminuyen con la implantación de seguridades, también conocidas como medidas, controles o contramedidas. Las seguridades pueden actuar contra la amenaza, la vulnerabilidad, el impacto o contra el propio riesgo. Sin embargo, no es factible atenuar todos los riesgos de forma completa, debido, en gran parte, al elevado costo económico y a las incertidumbres asociadas. Por tanto, siempre debe aceptarse algún riesgo residual.

2.5.2 Ingeniería

El proceso de ingeniería de seguridad se desarrolla junto con otras disciplinas de la ingeniería, para determinar e implementar soluciones a los problemas presentados por las amenazas y peligros (AREITIO, 2008, p. 8).

La creación de soluciones a los problemas de seguridad, implica identificar las posibles alternativas para evaluarlas posteriormente, y así, determinar cuál de ellas es la más adecuada para alcanzar los objetivos del negocio u organización. Como se ilustra en la figura, una vez identificadas las necesidades de seguridad, se identifica y se sigue la pista de los requisitos específicos (AREITIO, 2008, p. 8).

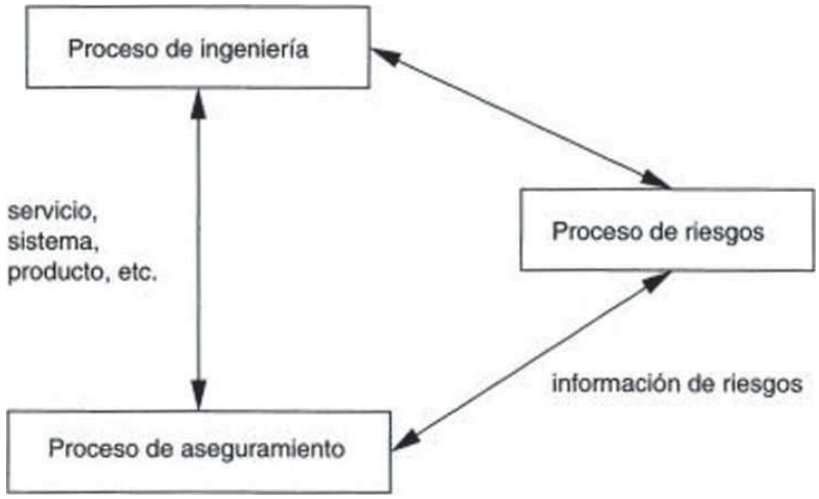


Ilustración 2.3Áreas de proceso de la seguridad.

Fuente: AREITIO (2008, p. 9).

A lo largo del ciclo de vida del sistema, la ingeniería de seguridad se encarga de garantizar que los productos y sistemas se encuentran configurados adecuadamente en relación a los riesgos percibidos, lo que se conoce como seguridad proactiva, asegurando que los nuevos riesgos no conviertan al sistema en inseguro al operar.

2.5.3 Aseguramiento

El proceso de aseguramiento es un elemento muy importante de la ingeniería de seguridad, que se define como el grado de confianza que satisfacen los requisitos de seguridad. Existen numerosas formas de garantizar el cumplimiento de los requisitos de seguridad. Todo modelo maduro de seguridad contribuye a un aspecto, que es la confianza en que los resultados han de repetirse cuando sea necesario durante el proceso de ingeniería de seguridad, es decir, que las medidas implementadas no tienen que crearse cada vez que se manifieste una amenaza (AREITIO, 2008, p. 9).

En la siguiente figura se muestra el esquema de las fases del proceso de aseguramiento.

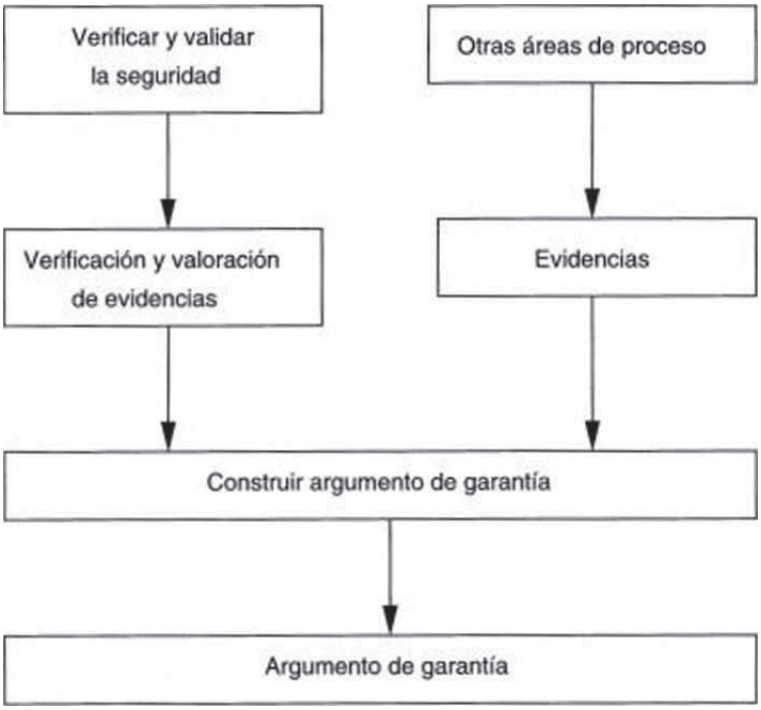


Ilustración 2.4Esquema del Proceso de Aseguramiento de la seguridad.

Fuente: AREITIO (2008, p. 10).

El aseguramiento no añade ningún control adicional al cálculo de riesgos relacionados con la seguridad, pero proporciona la confianza en que las seguridades implementadas reducirán el riesgo anticipado. El aseguramiento, también puede entenderse como la confianza en que las seguridades funcionarán como se pensaron. Esta confianza se deriva de las dos propiedades del aseguramiento, la corrección y la eficiencia. La solidez de los mecanismos, también desempeña una parte en la seguridad, pero depende del nivel de protección y de aseguramiento buscados.

El aseguramiento, a menudo, se comunica en forma de argumento, que incluye un conjunto de declaraciones acerca de las propiedades del sistema.

2.6 ELEMENTOS DE GESTIÓN DE LA SEGURIDAD

En el proceso de gestión de la seguridad de los sistemas de información hay una serie de elementos involucrados como son:



Ilustración 2.5 Elementos del proceso de gestión de la seguridad.

Fuente: AREITIO, 2008, p. 21.

La relación existente entre estos componentes se muestra en la siguiente figura.



Ilustración 2.6 Relación entre los elementos de la Gestión de la Información.

Fuente: AREITIO (2008, p. 22).

En este punto, es importante acotar que esta relación entre los elementos de la Gestión de la Información puede aportar un valor agregado a la organización como tal, al implementarse las respectivas seguridades del caso. Entre dichas ventajas, sobresalen las siguientes:

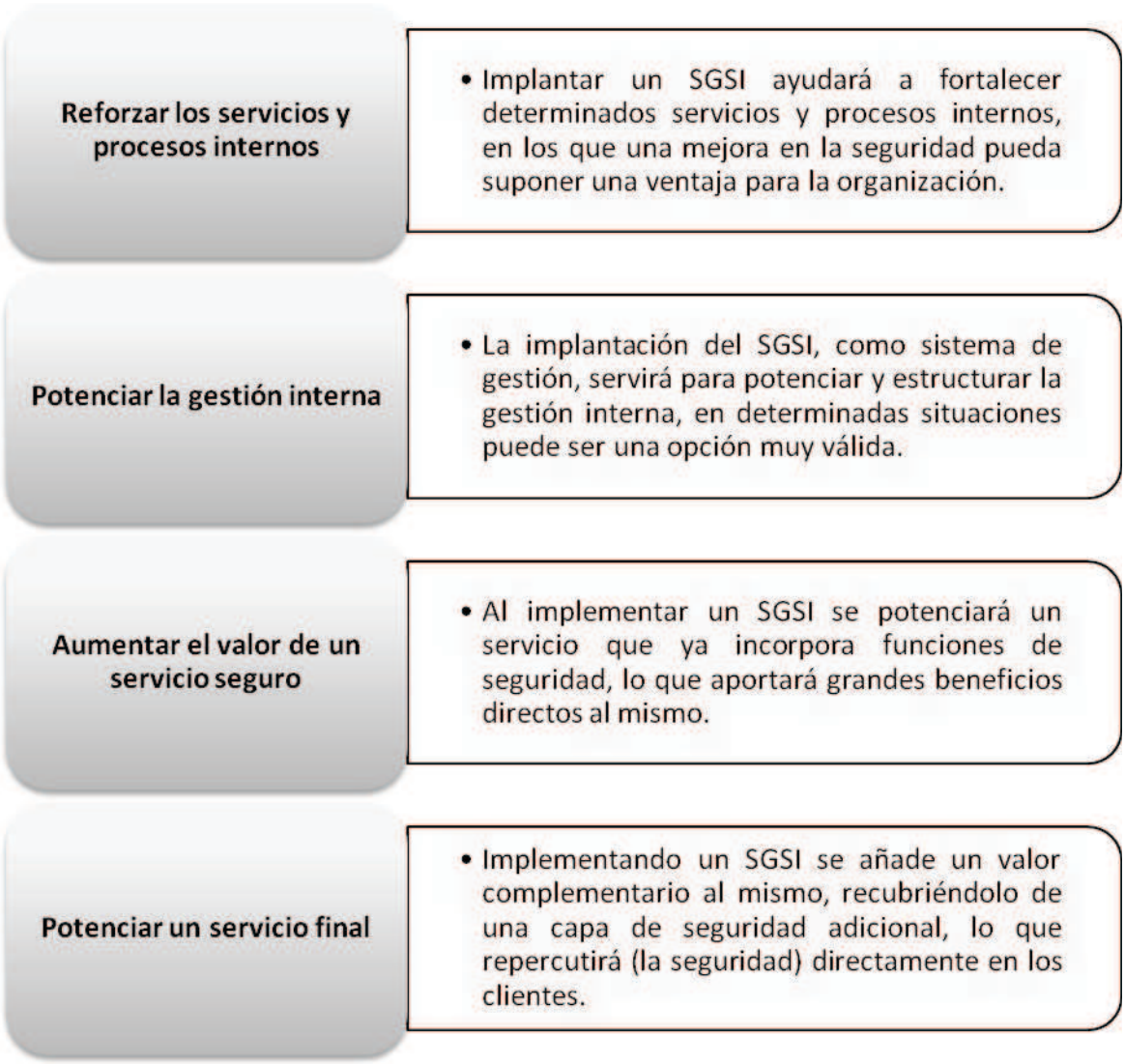


Ilustración 2.7 Valor agregado de la implementación de la seguridad de la información.

Elaborado: Autor.

2.7 DIFERENCIAS CON SEGURIDAD INFORMÁTICA

A primera vista "Seguridad de la Información" y "Seguridad Informática" pueden parecer exactamente lo mismo, sobre todo si se tiene en cuenta que el desarrollo y la evolución de la tecnología tienden hacia el modelo de "digitalizar" y "manejar" cualquier tipo de información mediante un sistema informático. No obstante, aunque están destinados a vivir en armonía y trabajar conjuntamente, cada uno de las áreas de Seguridad tiene objetivos y actividades diferentes (SEGURIDAD PARA TODOS, 2013).

La seguridad informática, se basa en la protección de la infraestructura computacional y todo lo relacionado con ésta. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. Es decir, comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore y signifique un riesgo si ésta llega a manos de otras personas. Se conoce como información privilegiada o confidencial.

Es así, que la Seguridad de la Información se fundamenta en el análisis de los riesgos, de las amenazas, de los escenarios, de las buenas

prácticas y esquemas normativos, que exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información.

Por tanto, la Seguridad Informática (IT Security) se describe como la distinción táctica y operacional de la Seguridad, mientras la Seguridad de la Información (Information Security) sería la línea estratégica de la Seguridad. IT Security sería la disciplina que se encargaría de llevar a cabo las soluciones técnicas de protección de la información (SEGURIDAD PARA TODOS, 2013).

La siguiente ilustración muestra en detalle el campo de acción de los dos tipos de seguridad mencionadas:

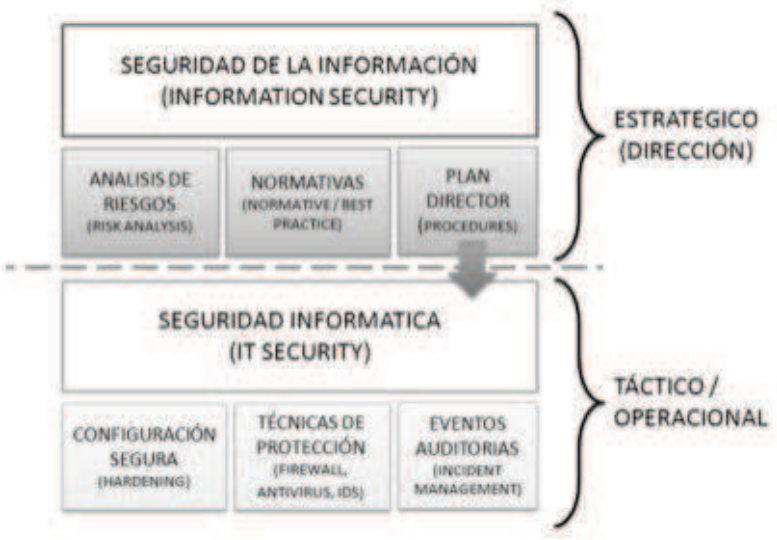


Ilustración 2.8 Campos de Acción de la Seguridad de la Información y de la Informática.

Fuente: SEGURIDAD PARA TODOS (2013).

Finalmente, es importante acotar que el concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

3 CAPÍTULO 2: NORMAS ISO

3.1 ISO

3.1.1 Definición de la ISO

ISO (Organización Internacional de Normalización) es el mayor desarrollador voluntario mundial de Normas Internacionales. Las Normas Internacionales dan las especificaciones del arte de productos, servicios y buenas prácticas, ayudando a hacer que la industria sea más eficiente y eficaz. Dichas normas son desarrolladas a través de un consenso global, que ayudan a eliminar las barreras al comercio internacional (ISO, s.f.a).

3.1.2 Historia de la ISO

La historia de ISO comenzó en 1946 cuando los delegados de 25 países se reunieron en el Instituto de Ingenieros Civiles en Londres y decidieron crear una nueva organización internacional para facilitar la coordinación y unificación de normas industriales internacionales. En febrero de 1947 la nueva organización, ISO, comenzó oficialmente sus operaciones.

Desde entonces, se han publicado más de 19.500 normas internacionales que abarcan casi todos los aspectos de la tecnología y la fabricación (ISO, s.f.a).

Hoy cuenta con miembros de 163 países y 3.368 organismos técnicos para cuidar de elaboración de normas.

3.1.3 Beneficios de las Normas Internacionales ISO

Las Normas Internacionales ISO garantizan que los productos y servicios sean seguros, fiables y de buena calidad. Para las empresas, son herramientas estratégicas que reducen los costos, disminuyendo al mínimo los desechos y los errores, y aumentando la productividad. Además, las ISO ayudan a las empresas a acceder a nuevos mercados, nivelar el campo de juego para los países en desarrollo y facilitar el comercio mundial libre y justo (ISO, s.f.a).

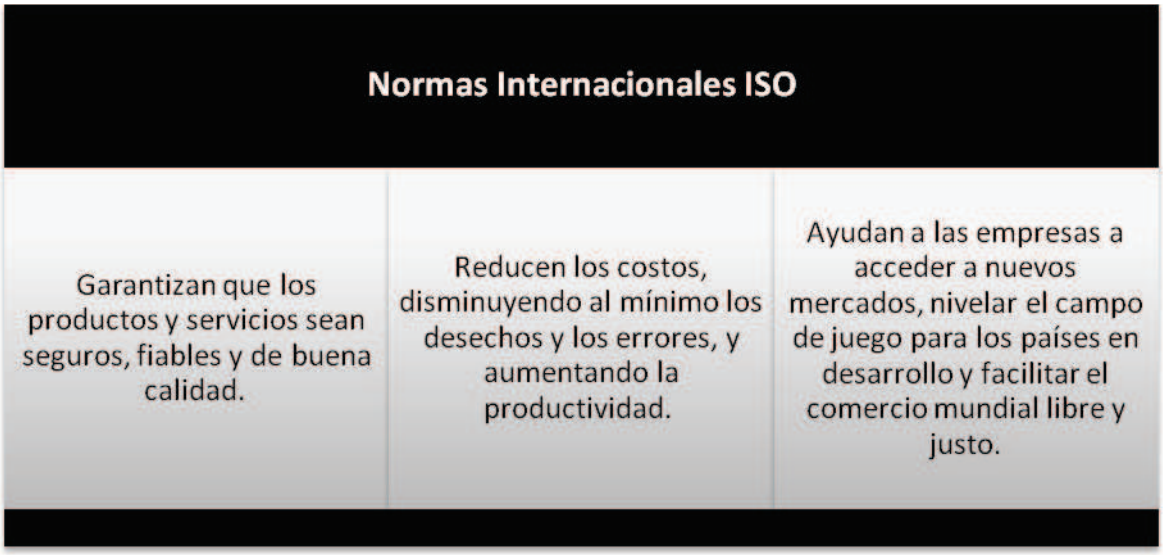


Ilustración 3.1 Beneficios de las ISO

Fuente: ISO (s.f.a).

3.1.4 Procedimiento para el Desarrollo de las Normas ISO

Una norma internacional es el resultado de un acuerdo entre los organismos miembros de ISO. Se puede utilizar como tal, o puede ser implementado a través de la incorporación en las normas nacionales de diferentes países. Es importante mencionar que las Normas Internacionales ISO son desarrolladas por los comités técnicos de ISO (TC) y subcomités (SC) por un proceso de seis pasos, los cuales abarcan:

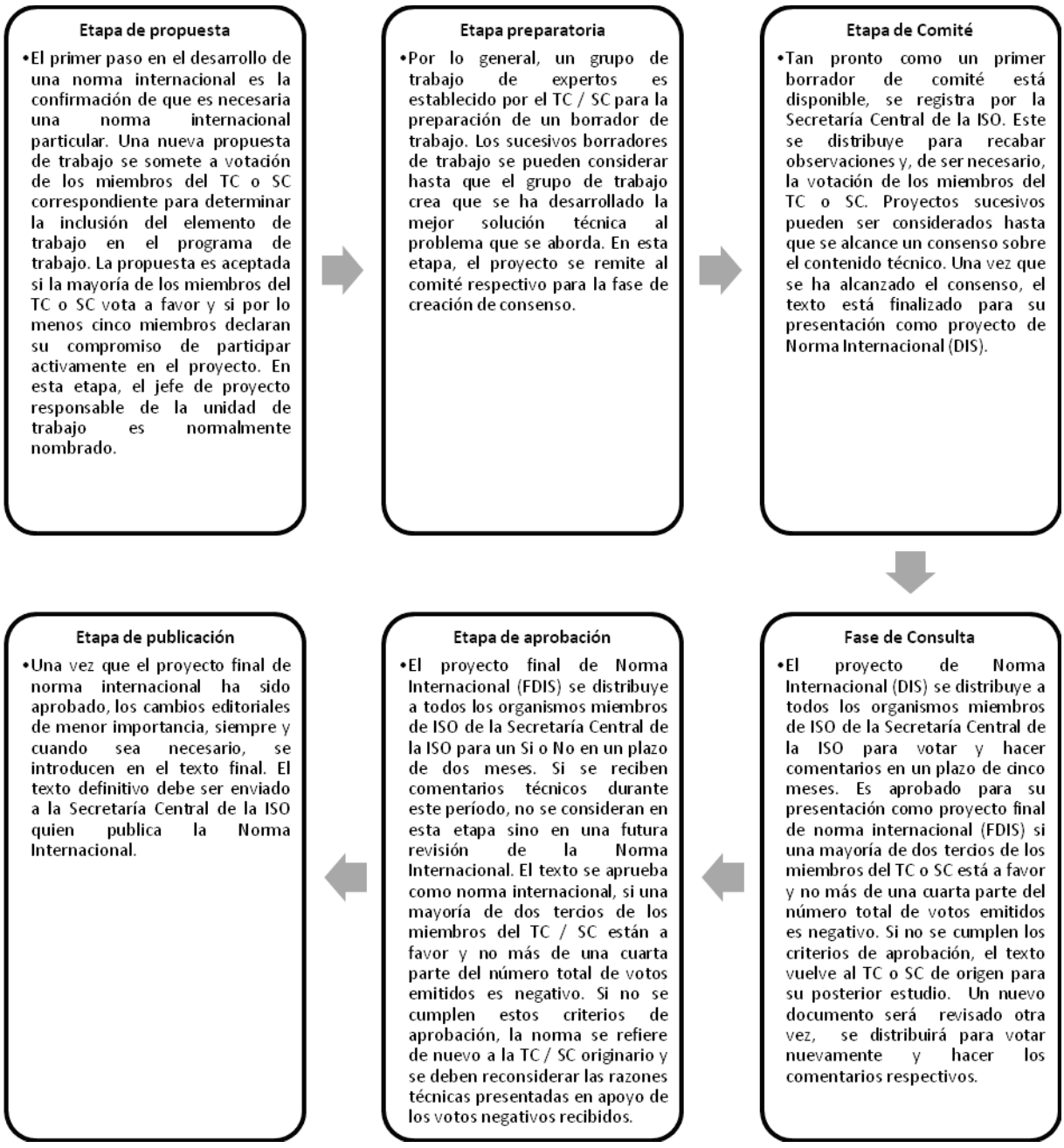


Ilustración 3.2 Proceso para el desarrollo de las Normas ISO.

Fuente: ISO (s.f.b).

En conclusión, la norma ISO es desarrollada por un grupo de expertos, dentro de un comité técnico. Una vez se ha establecido la necesidad de una norma, estos expertos se reúnen para discutir y negociar un proyecto. Tan pronto como un proyecto se ha desarrollado, se comparte con los miembros de la ISO y se pide hacer comentarios y votar por su aprobación. Si se llega a un consenso el proyecto se convierte en un estándar ISO, si no se lo remite nuevamente al comité técnico para que realice más ediciones.

Los principios fundamentales aplicados en la elaboración de normas, son los siguientes:

1. Normas ISO responden a una necesidad en el mercado.
2. Las normas ISO se basan en la opinión mundial de expertos.
3. Las normas ISO son desarrolladas a través de un proceso de múltiples partes interesadas.
4. Las normas ISO están basados en un consenso (ISO, s.f.b).

3.2 FAMILIA DE LAS NORMAS ISO 27000

3.2.1 Definición de las Normas ISO 27000

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es un objetivo de primer nivel para la organización. Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

En este sentido, las Normas ISO 27000 son un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO, que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña; ante cualquier amenaza o vulnerabilidad (ISO27000, 2012a).

La serie de Normas ISO 27000 se denomina “Requisitos para la especificación de sistemas de gestión de la seguridad de la información (SGSI)” y proporciona un marco de estandarización para la seguridad de la

información para que sea aplicado en una organización o empresa y comprende un conjunto de normas sobre las siguientes materias:

- Sistema de gestión de la seguridad del información
- Valoración de riesgos
- Controles (GARCÍA &ALEGRE, 2011, p. 19).

En esta serie de normas los rangos de numeración reservados por ISO va del 27 000 al 27019 y del 27030 al 27044.

Publicada el 1 de Mayo de 2009 y revisada con una segunda edición de 01 de Diciembre de 2012. Esta norma proporciona una visión general de los estándares que componen la serie 27000, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción del ciclo Plan-Do-Check-Act y términos y definiciones que se emplean en toda la serie 27000 (ISO27000, 2012a).

3.2.2 Origen de las Normas ISO 27000

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution) es responsable de la publicación de importantes normas. En 1995 la norma BS 7799 de BSI apareció por primera vez, con objeto de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de la información.

La primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas, para la que no se establecía un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que estableció los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente. Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión. En 2005, con más de 1700 empresas certificadas en BS 7799-2, esta norma se publicó por ISO, con algunos cambios, como estándar ISO 27001. Al tiempo se revisó y actualizó ISO 17799. Esta última norma se renombró como ISO 27002 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

Asimismo, ISO ha continuado, y continúa aún, desarrollando otras normas dentro de la serie 27000 que sirvan de apoyo a las organizaciones en la interpretación e implementación de ISO/IEC 27001, que es la norma principal y única certificable dentro de la serie (ISO27000, 2012b).

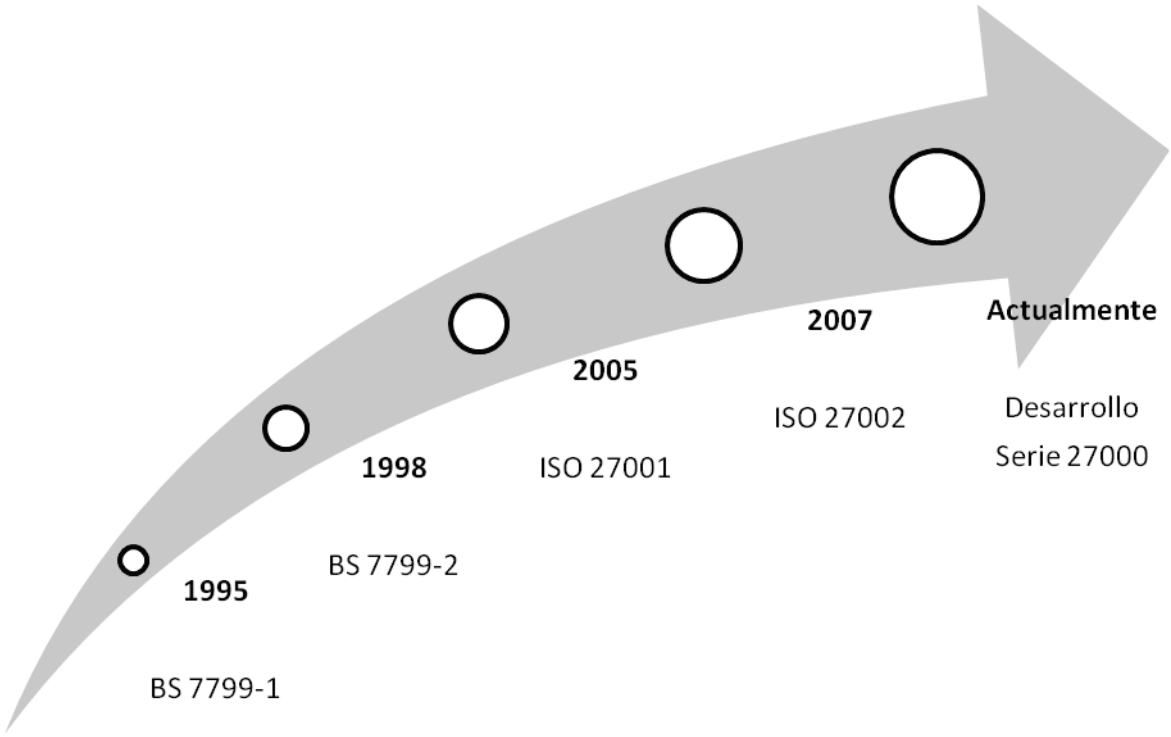


Ilustración 3.3 Historia de las Normas ISO 27000.

Fuente: ISO27000 (2012b).

3.2.3 Beneficios de las Normas ISO 27000

Entre los beneficios que las Normas ISO 27000 traen consigo, se destacan los siguientes:

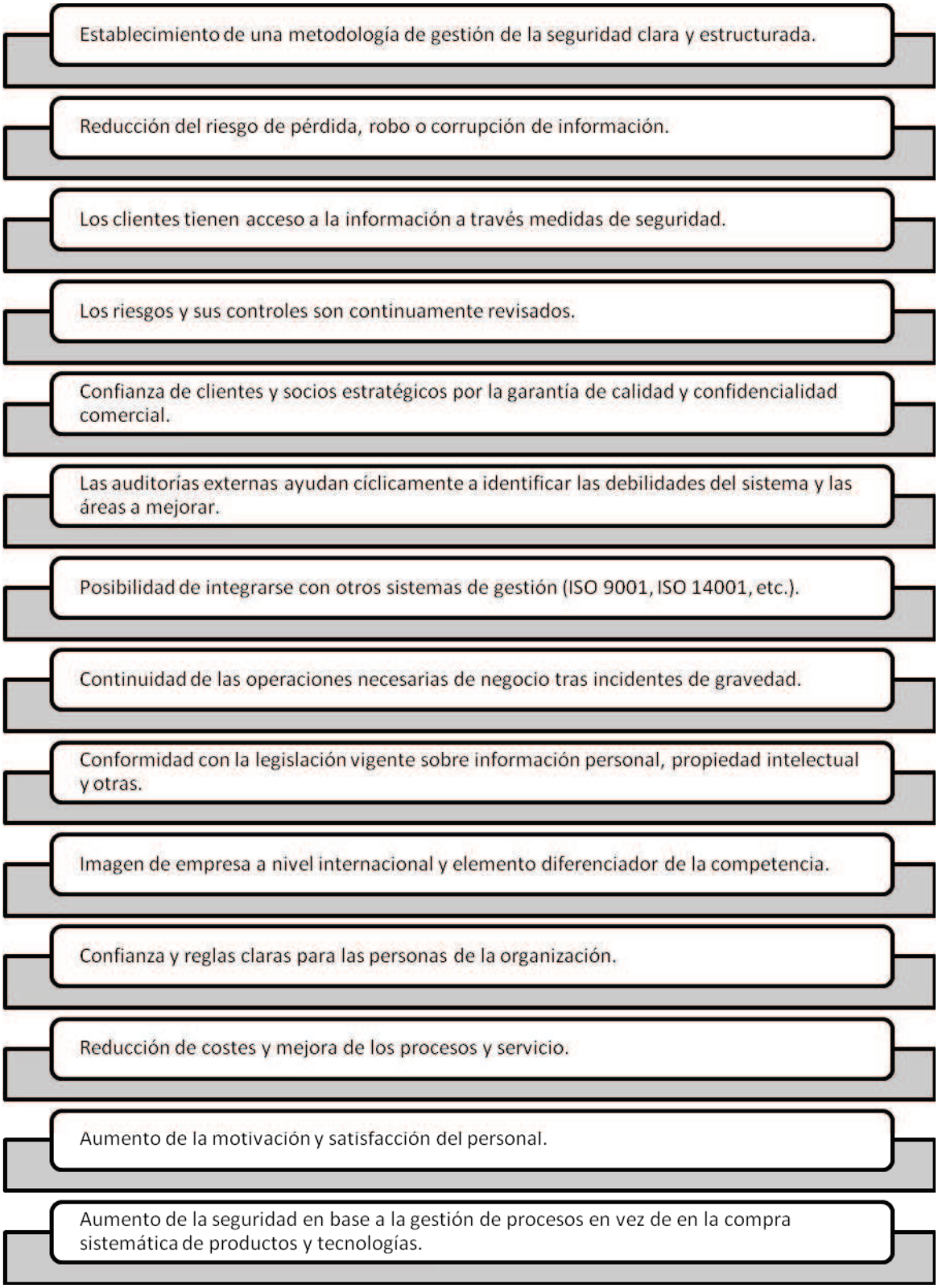


Ilustración 3.4 Beneficios de las Normas ISO 27000.

Fuente: ISO27000 (2012d).

En la siguiente ilustración, se muestra como las Normas ISO 27000, reducen los costos y aumentan los beneficios en las organizaciones que las implementan.



Ilustración 3.5 Beneficio Normas ISO 27000.

Fuente: ISO27000 (2012d).

3.2.4 Serie 27000

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares. La serie de normas de referencia y su estado de aprobación de Ediciones (entre paréntesis) a lo largo del tiempo se indican a continuación:



Ilustración 3.6 Desarrollo de Estándares de la Serie 27000.

Fuente: ISO27000 (2012c).

3.2.5 Contenido de la Serie 27000

Las Serio ISO 27000 está compuesta por varias Normas, a continuación se presenta un resumen de dichos estándares (ISO 27000, 2012d).

- ISO 27001

  Publicada el 15 de Octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. Actualmente, este estándar se encuentra en periodo de revisión en el subcomité ISO SC27, con fecha prevista de publicación para 2014.

- ISO/IEC 27002

  Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas

prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005. Actualmente, este estándar se encuentra en periodo de revisión en el subcomité ISO SC27, con fecha prevista de publicación de la segunda edición en Mayo de 2014.

- ISO/IEC 27003

  Publicada el 01 de Febrero de 2010. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

- ISO/IEC 27004

  Publicada el 15 de Diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida

aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.

- ISO/IEC 27005

  Publicada en segunda edición el 1 de Junio de 2011 (primera edición del 15 de Junio de 2008). No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Su primera publicación revisó y retiró las normas ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000.

- ISO/IEC 27006

  Publicada en segunda edición el 1 de Diciembre de 2011 (primera edición del 1 de Marzo de 2007). Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de

ISO 27001, pero no es una norma de acreditación por sí misma. Actualmente ha iniciado un nuevo periodo de revisión para una nueva versión 3.

- ISO/IEC 27007

  Publicada el 14 de Noviembre de 2011. No certificable. Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011.

- ISO/IEC TR 27008:

  Publicada el 15 de Octubre de 2011. No certificable. Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.

- ISO/IEC 27010

  Publicada el 20 de Octubre de 2012. Consiste en una guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores. ISO/IEC 27010:2012 es aplicable a todas las formas de intercambio y difusión de información sensible, tanto públicas como privadas, a nivel nacional e internacional, dentro de la misma industria o sector de mercado o entre sectores. En particular, puede ser aplicable a los intercambios de información y participación en relación con el suministro, mantenimiento y protección de una organización o de la infraestructura crítica de los estados y naciones.

- ISO/IEC 27011

  Publicada el 15 de Diciembre de 2008. Es una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002.

- ISO/IEC 27013

  Publicada el 15 de Octubre de 2012. Es una guía de implementación integrada de ISO/IEC 27001 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).

- ISO/IEC 27014

  En fase de desarrollo, con publicación prevista en 2013. Consistirá en una guía de gobierno corporativo de la seguridad de la información.

- ISO/IEC TR 27015

  Publicada el 23 de Noviembre de 2012. Es una guía de SGSI orientada a organizaciones del sector financiero y de seguros y como complemento a ISO/IEC 27002.

- ISO/IEC TR 27016

  En fase de desarrollo, con publicación prevista en 2013. Consistirá en una guía de valoración de los aspectos financieros de la seguridad de la información.

- ISO/IEC TS 27017

  En fase de desarrollo, con publicación prevista en 2013. Consistirá en una guía de seguridad para Cloud Computing.

- ISO/IEC 27018:

  En fase de desarrollo, con publicación prevista en 2013. Consistirá en un código de buenas prácticas en controles de protección de datos para servicios de computación en cloud computing.

- ISO/IEC TR 27019:

  En fase de desarrollo, con publicación prevista en 2013. Consistirá en una guía con referencia a ISO/IEC 27002 para el proceso de control de sistemas específicos al sector de la industria de la energía.

- ISO/IEC 27031

  Publicada el 01 de Marzo de 2011. No certificable. Es una guía de apoyo para la adecuación de las tecnologías de información y comunicación (TIC) de una organización para la continuidad del negocio. El documento toma como referencia el estándar BS 25777.

- ISO/IEC 27032

  Publicada el 16 de Julio de 2012. Proporciona orientación para la mejora del estado de seguridad cibernética, extrayendo los aspectos únicos de esa actividad y de sus dependencias en otros dominios de

seguridad, concretamente: Información de seguridad, seguridad de las redes, seguridad en Internet e información de protección de infraestructuras críticas (CIIP). Cubre las prácticas de seguridad a nivel básico para los interesados en el ciberespacio. Esta norma establece una descripción general de Seguridad Cibernética, una explicación de la relación entre la ciberseguridad y otros tipos de garantías, una definición de las partes interesadas y una descripción de su papel en la seguridad cibernética, una orientación para abordar problemas comunes de Seguridad Cibernética y un marco que permite a las partes interesadas a que colaboren en la solución de problemas en la ciberseguridad.

- ISO/IEC 27033

  Parcialmente desarrollada. Norma dedicada a la seguridad en redes, consistente en 7 partes: 27033-1, conceptos generales (publicada el 15 de Diciembre de 2009); 27033-2, directrices de diseño e implementación de seguridad en redes (publicada el 27 de Julio de 2012); 27033-3, escenarios de referencia de redes (publicada el 3 de Diciembre de 2010); 27033-4, aseguramiento de las comunicaciones entre redes mediante gateways de seguridad; 27033-5, aseguramiento de comunicaciones mediante VPNs (prevista para 2013); 27033-6, convergencia IP (prevista para 2013); 27033-7, redes inalámbricas (prevista para 2013).

- ISO/IEC 27034

  Parcialmente desarrollada. Norma dedicada la seguridad en aplicaciones informáticas, consistente en 5 partes: 27034-1, conceptos generales (publicada el 21 de Noviembre de 2011); 27034-2, marco normativo de la organización (sin previsión de publicación); 27034-3, proceso de gestión de seguridad en aplicaciones (sin previsión de publicación); 27034-4, validación de la seguridad en aplicaciones (sin previsión de publicación); 27034-5, estructura de datos de protocolos y controles de seguridad de aplicaciones (sin previsión de publicación).

- ISO/IEC 27035

  Publicada el 17 de Agosto de 2011. Proporciona una guía sobre la gestión de incidentes de seguridad en la información.

- ISO/IEC 27036

  En fase de desarrollo, con publicación prevista en 2013. Consistirá en una guía en cuatro partes de seguridad en las relaciones con proveedores: 27036-1, visión general y conceptos; 27036-2, requisitos comunes; 27036-3, seguridad en la cadena de suministro TIC; 27036-4, seguridad en outsourcing (externalización de servicios).

- ISO/IEC 27037

  Publicada el 15 de Octubre de 2012. Es una guía que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP, entre otros dispositivos y para que puedan ser utilizadas con valor probatorio y en el intercambio entre las diferentes jurisdicciones.

- ISO/IEC 27038

  En fase de desarrollo, con publicación prevista en 2013. Consistirá en una guía de especificación para seguridad en la redacción digital.

- ISO/IEC 27039

  En fase de desarrollo, con publicación prevista en 2013. Consistirá en una guía para la selección, despliegue y operativa de sistemas de detección y prevención de intrusión (IDS/IPS).

- ISO/IEC 27040

  En fase de desarrollo, con publicación prevista no antes de 2014. Consistirá en una guía para la seguridad en medios de almacenamiento.

- ISO/IEC 27041

  En fase de desarrollo, con publicación prevista no antes de 2014. Consistirá en una guía para la garantizar la idoneidad y adecuación de los métodos de investigación.

- ISO/IEC 27042

  En fase de desarrollo, con publicación prevista no antes de 2014. Consistirá en una guía con directrices para el análisis e interpretación de las evidencias digitales.

- ISO/IEC 27043

  En fase de desarrollo, con publicación prevista no antes de 2014. Desarrollará principios y procesos de investigación.

- ISO/IEC 27044

  En fase de desarrollo, con publicación prevista no antes de 2014. Gestión de eventos y de la seguridad de la información - Security Information and Event Management (SIEM).

- ISO 27799

  Publicada el 12 de Junio de 2008. Es una norma que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002, en cuanto a la seguridad de la información sobre los datos de salud de los pacientes. Esta norma, al

contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215.

3.3 Norma ISO 27001

3.3.1 Definición de la ISO 270001

La Norma ISO 27001 es la única norma internacional auditable que precisa los requisitos para una adecuada gestión de la seguridad de la información (BSI, 2013).

Esta norma se ha concebido para garantizar la selección de controles de seguridad adecuados y proporcionales. Esto ayuda a proteger los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes.

La norma ISO 27001 define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información. La ISO 27001 es para la seguridad de la información lo mismo que la ISO 9001 es para la calidad: es una norma redactada por los mejores especialistas del

mundo en el campo de seguridad de la información y su objetivo es proporcionar una metodología para la implementación de la seguridad de la información en una organización. También permite que una organización sea certificada, lo cual significa que una entidad de certificación independiente ha confirmado que la seguridad de la información se ha implementado en esa organización de la mejor forma posible (IS & BCA, 2013).

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información. Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías (ISO27000, 2012e).

3.3.2 Componentes básicos de la ISO 270001

El concepto básico que sustenta el SGSI es la seguridad de la información. Aunque es un concepto difícil de precisar por todos los elementos que implica, generalmente se acepta que son tres los componentes de la seguridad de la información:

- Confidencialidad: Asegurar que la información es accesible sólo a las personas que están autorizadas para tener acceso.
- Integridad: Salvaguardar la precisión y totalidad de la información y los métodos del procesamiento.
- Disponibilidad: Asegurar que los usuarios autorizados tienen acceso a la información y los activos asociados (ATEHORTÚA, BUSTAMANTE& VALENCIA, 2008, p.p. 31-32).



Ilustración 3.7 Componentes básicos del SGSI.

Elaborado: Autor.

3.3.3 Estructura del Modelo de SGSI

El modelo del SGSI ISO 27001 inicia con la definición del alcance del sistema determinando las áreas de procesos de la organización en los que se va a aplicar dicho sistema. Generalmente se eligen las áreas más críticas o vulnerables en materia de gestión de la información. Luego se debe formular divulgar una política de gestión de la seguridad de la información, que establezca los lineamientos generales que la organización debe tener en cuenta frente a los riesgos de la información, considerando en ello los riesgos legales, contractuales y propios de la empresa. El eje central de la planificación del SGSI consiste en identificar los riesgos de la información, en relación con las amenazas y los puntos vulnerables de la organización en cuanto a la confiabilidad, seguridad y disponibilidad de la información como tal. A partir de la identificación de estos riesgos, de su análisis y valoración, se definirán los planes de control o tratamiento del riesgo, que pretende llevarlo hasta un nivel aceptable o manejable por la entidad (ATEHORTÚA, BUSTAMANTE & VALENCIA, 2008, p.p. (p.p. 32-33).

La implementación se fundamenta en poner en práctica sus planes de control o tratamiento del riesgo. Incluye también la documentación y la aplicación de los procedimientos necesarios para aplicar tales controles, así como la formación y la concienciación de los empleados de la seguridad de la información y los controles que se han de aplicar. Un elemento importante es el de definir e implementar planes de detección y respuesta ante

incidentes de seguridad de la información, para reducir el impacto que tales incidentes pueden tener en operación de la organización (ATEHORTÚA, BUSTAMANTE & VALENCIA, 2008, p.p. (p.p. 32-33).

La verificación incluye la medición del desempeño del SGSI, la evaluación de los riesgos y la eficacia de los controles implementados, la realización de auditorías internas del sistema y la revisión del mismo por parte de la dirección. De estas acciones se desprende el mejoramiento, que incluye la actualización de los planes de seguridad y la definición de implementación de las acciones correctivas y preventivas a que haya lugar (ATEHORTÚA, BUSTAMANTE & VALENCIA, 2008, p 33).

En la siguiente figura se representa gráficamente el modelo de la seguridad de la información anteriormente detallado.

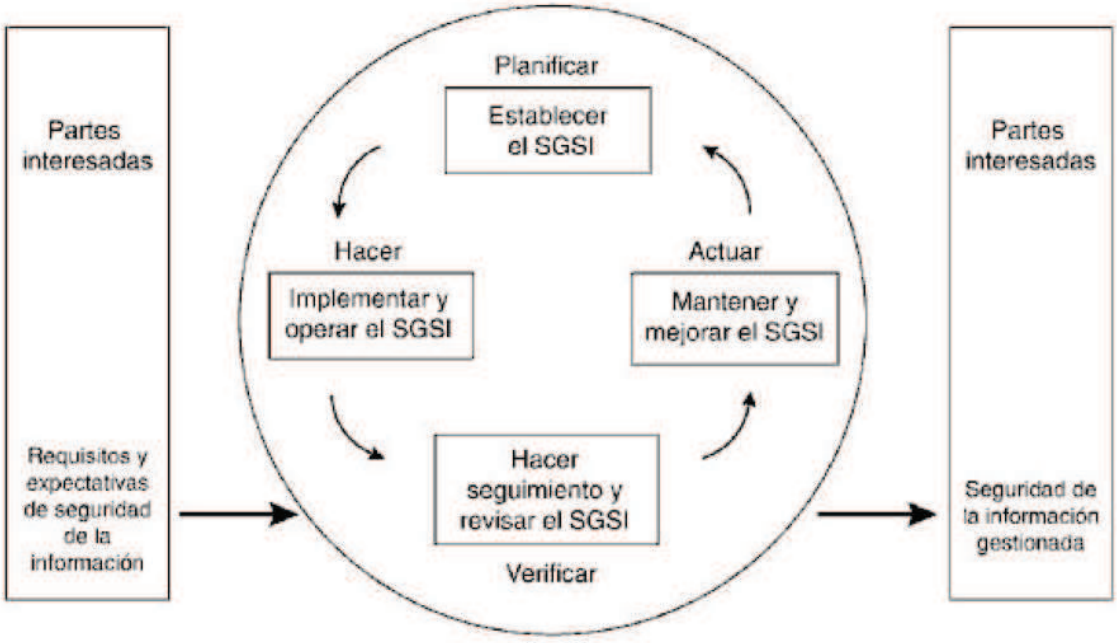


Ilustración 3.8 Modelo SGSI.

Fuente: ATEHORTÚA, BUSTAMANTE & VALENCIA (2008, p 33).

3.3.4 Fases del SGSI

La norma ISO 27001 determina cómo gestionar la seguridad de la información a través de un SGSI, conformado por cuatro fases que se deben implementar en forma constante para reducir al mínimo los riesgos sobre confidencialidad, integridad y disponibilidad de la información.

En la siguiente ilustración se muestran dichas fases:

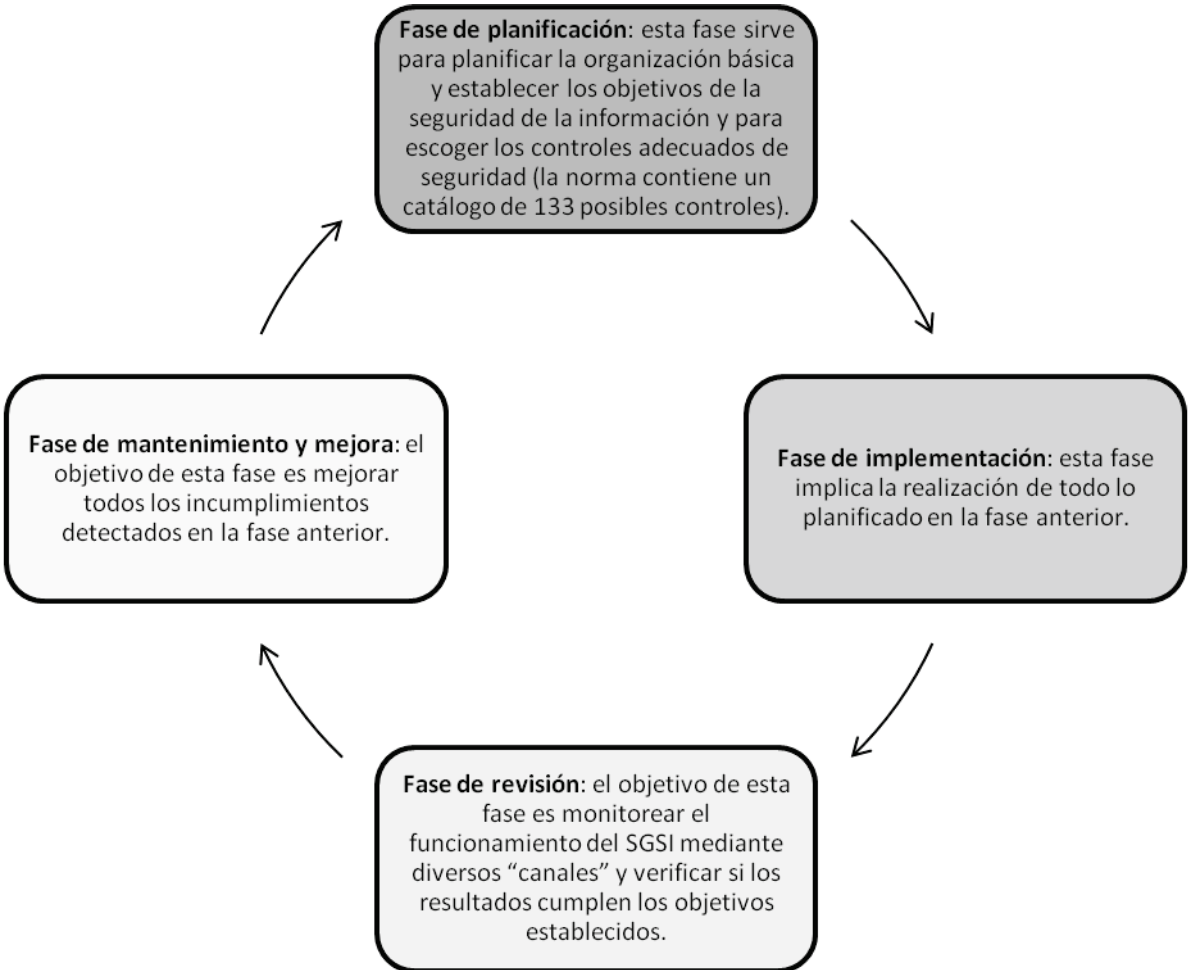


Ilustración 3.9 Fases del SGSI.

Fuente: IS & BCA (2013).

El ciclo de estas cuatro fases nunca termina, todas las actividades deben ser implementadas cíclicamente para mantener la eficacia del SGSI.

3.3.4.1 Fase de Planificación

Esta fase está formada por los siguientes pasos:

- Determinación del alcance del SGSI;
- Redacción de una Política de SGSI;
- Identificación de la metodología para evaluar los riesgos y determinar los criterios para la aceptabilidad de riesgos;
- Identificación de activos, vulnerabilidades y amenazas;
- Evaluación de la magnitud de los riesgos;
- Identificación y evaluación de opciones para el tratamiento de riesgos;
- Selección de controles para el tratamiento de riesgos;
- Obtención de la aprobación de la gerencia para los riesgos residuales;
- Obtención de la aprobación de la gerencia para la implementación del SGSI;
- Redacción de una declaración de aplicabilidad que detalle todos los controles aplicables, determine cuáles ya han sido implementados y cuáles no son aplicables (IS & BCA, 2013).

3.3.4.2 Fase de Implementación

Esta fase incluye las siguientes actividades:

- Redacción de un plan de tratamiento del riesgo que describe quién, cómo, cuándo y con qué presupuesto se deberían implementar los controles correspondientes;
- Implementación de un plan de tratamiento del riesgo;
- Implementación de los controles de seguridad correspondientes;

- Determinación de cómo medir la eficacia de los controles;
- Realización de programas de concienciación y capacitación de empleados;
- Gestión del funcionamiento normal del SGSI;
- Gestión de los recursos del SGSI;
- Implementación de procedimientos para detectar y gestionar incidentes de seguridad (IS & BCA, 2013).

3.3.4.3 Fase de Verificación

Esta fase incluye lo siguiente:

- Implementación de procedimientos y demás controles de supervisión y control para determinar cualquier violación, procesamiento incorrecto de datos, si las actividades de seguridad se desarrollan de acuerdo a lo previsto, etc.;
- Revisiones periódicas de la eficacia del SGSI;
- Medición la eficacia de los controles;
- Revisión periódica de la evaluación de riesgos;
- Auditorías internas planificadas;
- Revisiones por parte de la dirección para asegurar el funcionamiento del SGSI y para identificar oportunidades de mejoras;

- Actualización de los planes de seguridad para tener en cuenta otras actividades de supervisión y revisión;
- Mantenimiento de registros de actividades e incidentes que puedan afectar la eficacia del SGSI (IS & BCA, 2013).

3.3.4.4 Fase de Mantenimiento y mejora

Esta fase incluye lo siguiente:

- Implementación en el SGSI de las mejoras identificadas;
- Toma de medidas correctivas y preventivas y aplicación de experiencias de seguridad propias y de terceros;
- Comunicación de actividades y mejoras a todos los grupos de interés;
- Asegurar que las mejoras cumplan los objetivos previstos (IS & BCA, 2013).

4 CAPITULO 3: SISTEMA DE GESTIÓN

4.1 PYMES ECUATORIANAS

4.1.1 Introducción

Se conoce como PYMES al conjunto de pequeñas y medianas empresas que de acuerdo a su volumen de ventas, capital social, cantidad de trabajadores, y su nivel de producción o activos presentan características propias de este tipo de entidades económicas (SRI, 2010).

En Ecuador, las pequeñas y medianas empresas realizan diferentes tipos de actividades económicas, entre las que se destacan las siguientes:

- Comercio al por mayor y al por menor.
- Agricultura, silvicultura y pesca.
- Industrias manufactureras.
- Construcción.
- Transporte, almacenamiento, y comunicaciones.
- Bienes inmuebles y servicios prestados a las empresas.
- Servicios comunales, sociales y personales (SRI,2010).

El actual mundo globalizado genera mercados altamente competitivos, lo que exige a las Pymes a buscar estrategias que le permitan mantener este ritmo acelerado. Una Pyme en crecimiento necesita no solo promover su negocio y mejorar su productividad, en este sentido el comercio electrónico es una gran herramienta a utilizar, logrando así ser más competitivas y abarcar un mercado más extenso.

Por lo tanto, contar con herramientas adecuadas no solo permite que una Pyme optimice sus procesos, sino también, que ayude a su consolidación; por esta razón, las Pymes intentan aprovechar la tecnología y los recursos actualmente disponibles para este fin, sin embargo son grandes los conflictos a superar, más si se trata de la seguridad de la información.

Como solución a este problema en particular, se presenta un sistema de gestión de la seguridad de la información para comercio electrónico, el cual contiene las principales políticas de seguridad de la información, bajo las Normas ISO 27001, y que sirva como plan de acción para el mejoramiento de la seguridad de la información en las Pymes de la ciudad de Quito, de acuerdo a la realidad de las mismas; a fin de alcanzar la eficiencia y eficacia, en las actividades de resguardo y protección de la información, en especial frente a posibles hackeos.

4.1.2 Procesos

Los procesos de negocio comunes en una Pyme dependen de la actividad comercial a la que se dedique la Pyme, sea esta de productos o servicios. Frecuentemente se identifican tres procesos básicos:

- Proceso de Compra
- Proceso de Venta
- Proceso de Producción (si fuera una empresa Manufacturera).

A continuación se muestran los diagramas de flujo correspondientes a los procesos antes mencionados:

PROCESO DE VENTA

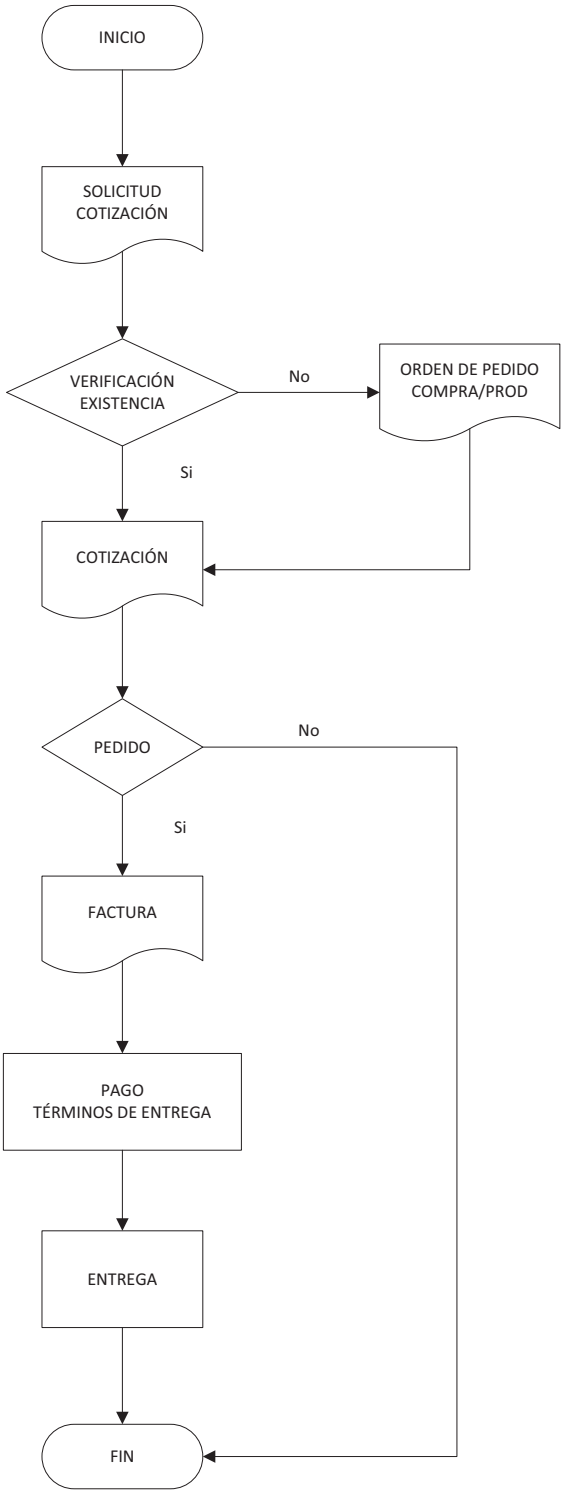


Ilustración 4.1. Proceso de Venta.

Elaborado: Autor.

PROCESO DE COMPRA

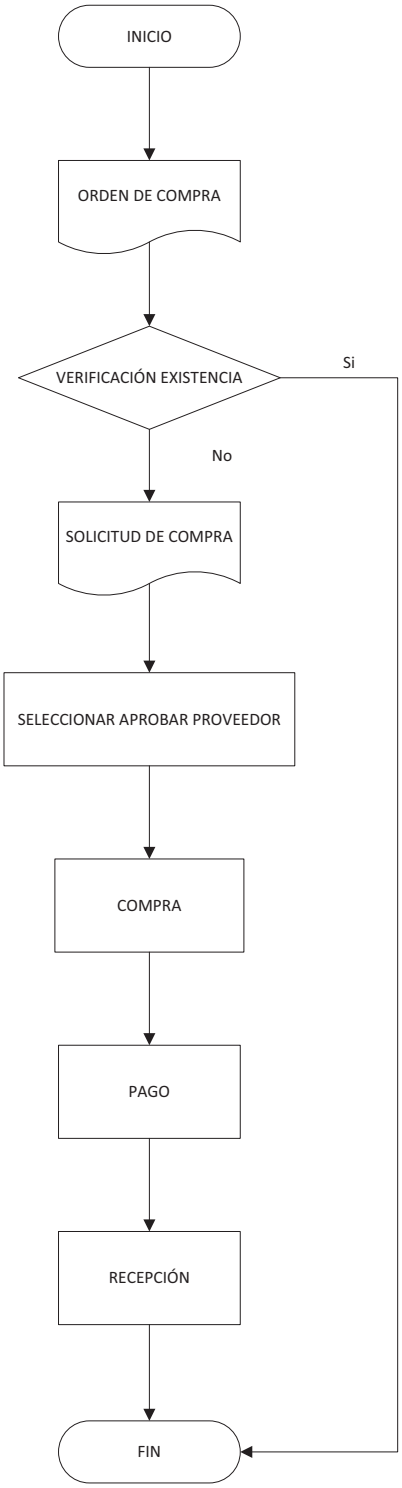


Ilustración 4.2. Proceso de Compra.

Elaborado: Autor

PROCESO DE PRODUCCIÓN

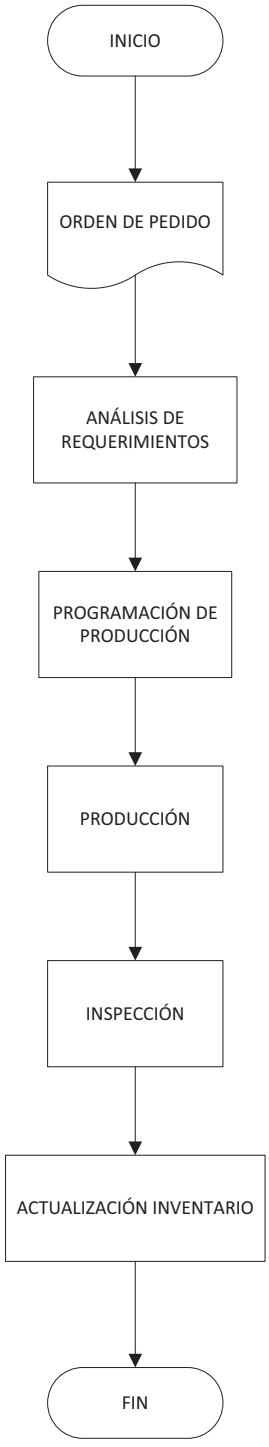


Ilustración 4.3. Proceso de Producción.

Elaborado: Autor.

Específicamente al hablar del comercio electrónico, objeto de estudio de esta disertación, se tiene que el flujo operativo entre el cliente y la Pyme se da de la siguiente manera:

1. El usuario ingresa a la Página Web de la Pyme, para buscar un producto.
2. El comprador debe elegir el producto que desea.
3. El carrito de compras se llena con los productos elegidos.
4. Se realizan los cálculos del valor total, considerando los impuestos respectivos y el costo del envío.
5. Para realizar la compra, el cliente debe ingresar el usuario y la contraseña respectiva, si ya se ha registrado anteriormente; caso contrario, debe llenar el formulario de suscripción.
6. Cuando el comprador ha enviado todos sus datos, mediante el sistema de pago (empresa validadora), se concreta la transacción.

Es importante mencionar, este proceso operativo se anexa al proceso de ventas como tal.

En el siguiente Flujograma se ilustra este proceso en particular.

PROCESO DE COMERCIO ELECTRÓNICO

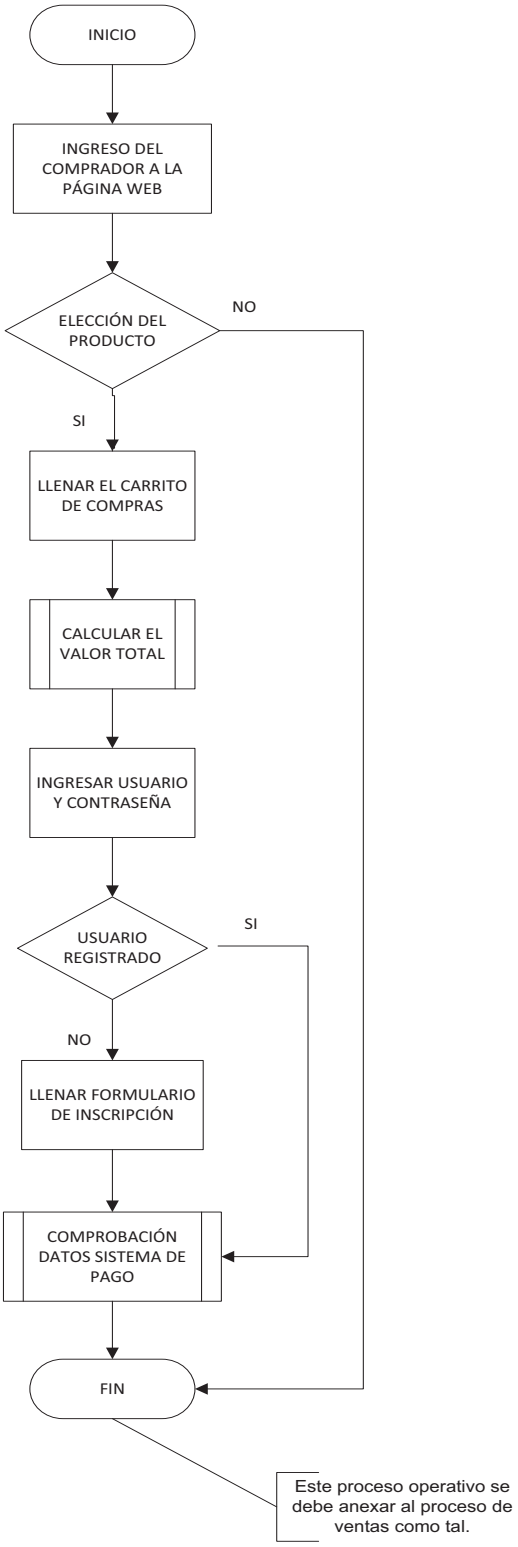


Ilustración 4.4 Proceso de eCommerce.

Elaborado: Autor.

4.2 GENERALIDADES

En este punto, es necesario unificar los aspectos relacionados al concepto de “comercio electrónico”; es este sentido, se hace énfasis en cuanto a las modalidades de comercio electrónico, pues un error frecuente es considerar que se trata de un sistema que permite a las organizaciones ofrecer sus productos y servicios a clientes particulares cuando, en realidad, en función del tipo de agente que interviene en la transacción se pueden distinguir diferentes relaciones:

- **Empresa - Empresa o B2B**: cualquier intercambio que tenga lugar entre dos organizaciones. Este tipo de comercio electrónico proporciona nuevos canales de comunicación, intercambio, selección de información y facilita la implementación de estrategias de cooperación, además de mecanismos transaccionales para la finalización de la transacción en un entorno 100% online.
- **Empresa - Consumidor final o B2C**: intercambio de información, bienes o servicios entre una organización y sus públicos externos (clientes, clientes potenciales, empleados, accionistas, etc.).
- **Empresa - Administración o B2A**: relación a través de redes de telecomunicación entre una organización y las Administraciones Públicas. El desarrollo de esta modalidad puede conducir a la adopción de sistemas de comercio electrónico de forma obligatoria (por ejemplo, mediante la obligación de prestar los servicios de forma puramente online o de facturar electrónicamente.

- **Ciudadano - Administración C2G**: relación entre los ciudadanos y las Administraciones Públicas a través de redes de telecomunicación para la obtención de información, acceso a servicios, pago de impuestos, realización de notificaciones, etc. (Programa para el Desarrollo del Comercio Electrónico en la Comunidad de Madrid, s.f.).

Cabe acotar, que este trabajo se encasilla en el tipo B2C (Comercio - vendedor a Consumidor final – comprador.

4.3 PROCEDIMIENTO

El campo de la Seguridad de la Información incluye la tecnología, que se preocupa por la seguridad de los sistemas TI y los datos almacenados en los mismos. Únicamente con la compra de firewalls y antivirus no es suficiente. Para garantizar una protección fiable se necesita más bien una planificación estructurada, así como un control de todas las medidas de seguridad.

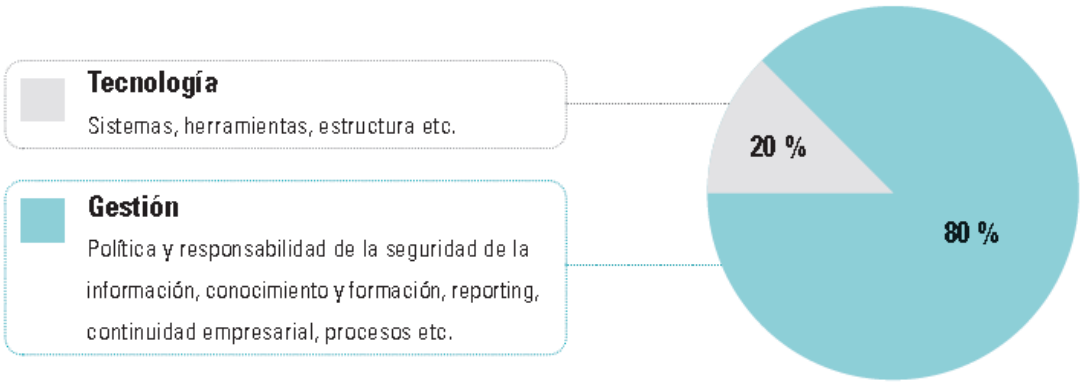


Ilustración 4.5 Como garantizar la seguridad de la información.

Fuente: TÜV SÜD IBERIA (s.f.).

En base al estándar internacional ISO/IEC 27001: 2005 (Primera Edición, 2005 - 10 – 15), el cual se adjunta en su totalidad en el Anexo 2 y considerando que el Sistema de Gestión de la Seguridad de la Información (SGSI) sigue un enfoque basado en procesos que utilizan el ciclo de mejora continua o de Deming, que consiste en Planificar - Hacer - Verificar - Actuar, más conocido con el acrónimo en inglés PDCA (Plan - Do - Check - Act) y que también se fundamenta en la norma ISO/IEC 27002:2009, que recoge una lista de objetivos de control y controles necesarios para lograr cumplir con los objetivos de seguridad de la información (Asociación Española para la Calidad, 2013); para el desarrollo de la propuesta se tomará en cuenta el siguiente procedimiento:

- **Fase de Planificación** (Plan) -construir el SGSI-: Establecer la política, objetivos, procesos y procedimientos relativos a la gestión del riesgo y mejorar la seguridad de la información de la organización para ofrecer resultados de acuerdo con las políticas y objetivos generales de la organización.

- **Fase de Implementación** (Do) -implementar y gestionar el SGS-: Implementar y gestionar el SGSI de acuerdo a su política, controles, procesos y procedimientos.

- **Fase de Verificación y Seguimiento** (Check) -monitorizar y revisar el SGSI-: Medir y revisar las prestaciones de los procesos del SGSI.

- **Fase Mantenimiento y Mejora** (Act) -mantener y mejorar el SGSI-: Adoptar acciones correctivas y preventivas basadas en auditorías y revisiones internas ó en otra información relevante a fin de alcanzar la mejora continua del SGSI.

En conclusión, la propuesta se ejecutará en base al procedimiento mostrado en la siguiente Ilustración.

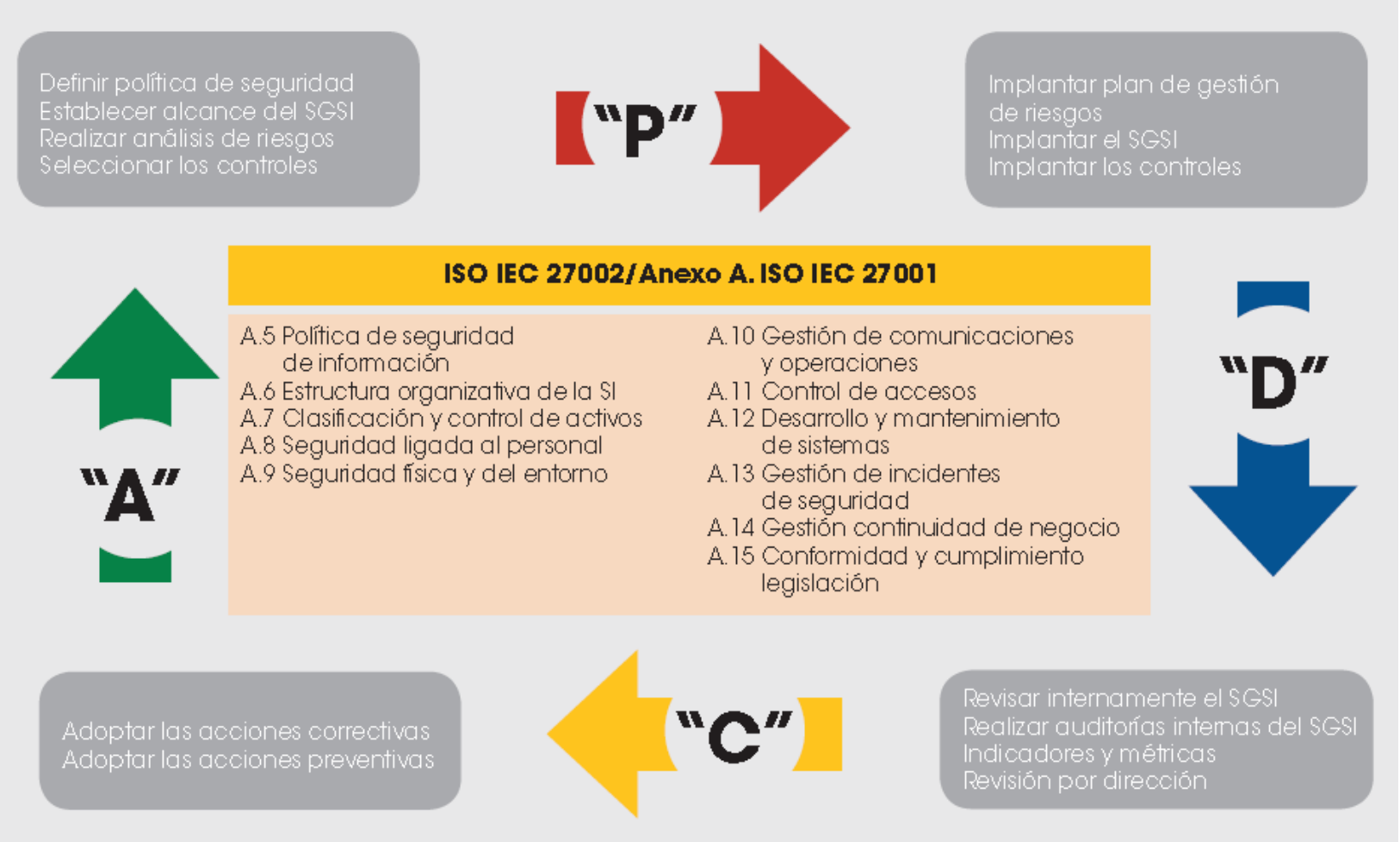


Ilustración 4.6Procedimiento SGI a seguir.

Fuente: ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD (2013).

Como se puede observar, en resumen la norma ISO / IEC 27001 consta de dos partes: el sistema de gestión y los controles necesarios que deben considerarse en cualquier caso.

4.4 DESARROLLO

En base a lo anteriormente mencionado, se han identificado seis pasos fundamentales a seguir en la implementación de un Sistema de Gestión de Seguridad de la Información para Pymes ecuatorianas, conforme a la ISO/IEC 27001:

1. Definición del alcance y los límites del SGSI.
2. Definición de la política de la seguridad de la información.
3. Identificación de los activos de la Pyme y sus riesgos asociados.
4. Control de riesgos.
5. Fijación de controles y objetivos de control.
6. Definición de la Declaración de la Aplicabilidad.

En estos pasos corresponden a la planificación como tal. A partir de dichos pasos se proponen las acciones a seguir en las siguientes fases (implementación, verificación y mantenimiento).

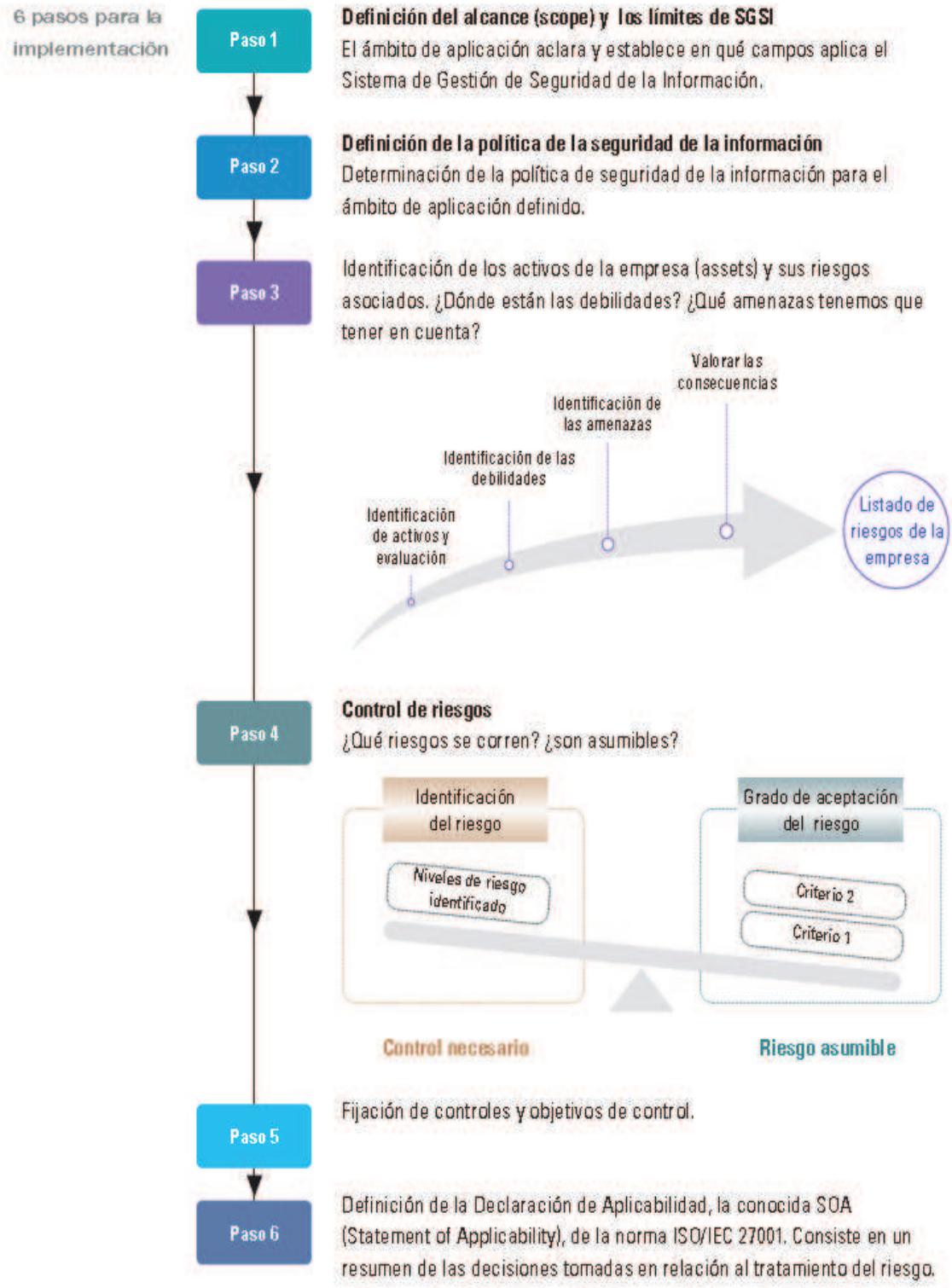


Ilustración 4.7 Pasos para la implementación de un SGSI.

Fuente: TÜV SÜD IBERIA (S.F.)

4.5 PROPUESTA

A continuación, se presenta la propuesta de un Sistema de Gestión de Seguridad de la Información para el comercio electrónico en Pymes ecuatorianas.

4.5.1 Fase de Planificación

4.5.1.1 Alcance y límite del SGSI

La presente propuesta cubrirá los aspectos de seguridad de los activos tangibles e intangibles participes en el comercio electrónico de una Pyme. Para esto, se adaptará la norma ISO 27001 en base a la realidad existente en una organización en particular, con un análisis de riesgos, identificación de amenazas y vulnerabilidades.

4.5.1.2 Políticas de Seguridad

4.5.1.2.1 <u>Ámbito</u>

La presente Política de Seguridad de la Información debe ser divulgada y cumplida por todo el personal vinculado al proceso de comercio electrónico.

4.5.1.2.2 Objetivo

Proteger los recursos utilizados en el comercio electrónico de una Pyme, frente a amenazas (internas o externas y/o deliberadas o accidentales), y así asegurar el cumplimiento de la confidencialidad, la integridad y la disponibilidad de la información.

4.5.1.2.3 Políticas de los activos de información

Propósito: Evitar riesgos potenciales de los activos de información, asociados a su accionar cotidiano, de manera accidental o intencionada, y que puedan ocasionar la interrupción de las actividades de una Pyme.
Acciones: • Se deben definir procedimientos eficaces para el rotulado y manejo de información, los mismos deben contemplar los recursos de información tanto en formatos físicos como electrónicos. • Todos los activos deben tener una persona responsable, quien será el encargado de la protección de los mismos. • El custodio de los activos debe definir que usuarios pueden acceder a los datos que estos contengan. • Los activos de información deben estar salvaguardados con cables de seguridad en todo momento para evitar pérdidas o robos. • Las estaciones de trabajo se deben mantener en estricto control, para lo cual deberá utilizar contraseñas de acceso a su computador y aplicaciones, evitando el acceso indebido a la información cuando el personal no se encuentre físicamente en su estación de trabajo. • Se debe controlar el mantenimiento preventivo del equipamiento informático de

acuerdo a las indicaciones de proveedores, el cual asegurará su disponibilidad e integridad permanentemente.

Tabla 4.1 Políticas de Seguridad de Activos.

Elaborado: Autor.

4.5.1.2.4 Políticas del personal

Propósito: Reducir los riesgos de error humano y definir mecanismos para el uso adecuado de recursos, así como las responsabilidades del personal en materia de seguridad de la información.
Acciones: • Asegurar que los usuarios autorizados tengan acceso a la información y sistemas asociados cuando se requiera. • Los usuarios son responsables de mantener la integridad de sus cuentas y proteger todas las credenciales de acceso. • No está permitido a los usuarios compartir cuentas o passwords con otras personas, romper seguridades. • No debe abusar de los recursos disponibles. • Se prohíbe el acceso a archivos de otros usuarios, a no ser que le sea permitido por parte del responsable del activo. • Si el usuario identifica que la cuenta y/o clave ha sido violada, debe contactar al departamento de IT el inconveniente y cambiar la contraseña. • Todo el personal es responsable del reporte de debilidades e incidentes de seguridad que oportunamente se detecten. • Es necesario establecer la responsabilidad sobre el cumplimiento de las

normas de seguridad de la información tanto de los empleados como del personal administrativo o de servicio, según corresponda. Los procesos contractuales deberán establecer las responsabilidades de cada empleado en lo que a seguridad de la información se refiere.

- Como parte de sus términos y condiciones iníciales de reclutamiento, los empleados deberán firmar un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información.
- Cada integrante de la Pyme deberá recibir una adecuada capacitación y actualización periódica en lo relacionado a la política y normas relacionadas a la seguridad. Esto incluirá los requerimientos de seguridad y las responsabilidades que cada usuario adquiere al iniciar sus labores.

Tabla 4.2Políticas de Seguridad del Personal.

Elaborado: Autor.

4.5.1.2.5 Políticas de seguridad física

Propósito: Prevenir e impedir accesos no autorizados, daños e interferencia a las instalaciones e información de una Pyme, de esta manera proteger el equipamiento e información crítica de la misma.

Acciones:

- Todos los empleados deben contar con una identificación que permita su ingreso a las instalaciones de la Pyme.
- En zonas altamente "sensibles" solo deberá transitar el personal autorizado para ese lugar.
- El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas, peligros ambientales, y las oportunidades de acceso no autorizado.
- La protección se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas.

• La Pyme debe utilizar perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información.

Tabla 4.3Políticas de Seguridad Física.

Elaborado: Autor.

4.5.1.2.6 Políticas de control de acceso e ingreso a los sistemas

Propósito: Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información en general, concienciando a los usuarios respecto de su responsabilidad frente a la utilización de los mismos.
Acciones: • Todos los usuarios deben ser autentificados. Cada usuario debe ser identificado por un nombre y pertenecer a un grupo dentro del sistema operativo o a un rol dentro de la base de datos. • Cuando un usuario ya no es parte del personal de la Pyme, su cuenta debe ser eliminada inmediatamente. • Los usuarios deben ser capaces únicamente de modificar los datos que les pertenecen, y sólo podrán consultar los datos siempre y cuando estos estén autorizados para hacerlo. • Sólo el administrador IT debe tener la capacidad de conectarse a los recursos del sistema en modo privilegiado para realizar tareas administrativas. • Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad, así mismo, será aprobado, controlado y registrado en detalle por los responsables de cada área. • Se debe definir un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a la información, limitando y controlando la asignación, uso de privilegios.

- A fin de mantener un control eficaz de acceso a los datos y servicios de información, el Propietario de la Información llevará a cabo un proceso formal, a intervalos regulares de no más de 6 meses, a fin de revisar los derechos de acceso de los usuarios.
- Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas y deben cumplir las directivas que se impartan a tal efecto.
- El responsable de la administración de los sistemas tiene que asegurar que la información esté disponible cuando sea necesario.
- La información confidencial debe manejarse bajo el criterio de acceso autorizado y no debe estar sujeta a cambios no autorizados.
- Cuando exista la necesidad de otorgar accesos especiales a la información confidencial, se llevará a cabo una evaluación de riesgos para identificar los requerimientos de controles específicos.

Tabla 4.4 Políticas de Control de Acceso e Ingreso a los Sistemas.

Elaborado: Autor.

4.5.1.2.7 Políticas de software

Propósito: Lograr niveles adecuados de integridad, confidencialidad y disponibilidad para todos los equipos e información relevante, mediante acciones generales en cada estación de trabajo, cuyo objeto principal es asegurar continuidad operacional de los procesos y servicios.

Acciones:

- Las estaciones de trabajo deben estar protegidas por software antivirus con capacidad de actualización automática en cuanto a firmas de virus. Los usuarios no están autorizados a deshabilitar este control.
- Los usuarios no deben instalar software en sus estaciones de trabajo, en los servidores de la red, o en otras máquinas, incluso si este software es libre o no licenciado; toda instalación de software debe hacerla un responsable del área de

Sistemas.

- No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor.
- Los programas de juegos no son permitidos en las estaciones de trabajo de los usuarios.
- Todo software desarrollado o adquirido debe ser validado previo a su uso.
- Se deberá mantener una base de datos actualizada que contenga un registro del software autorizado para su uso e instalación en la Pyme.

Tabla 4.5 Políticas de Software.

Elaborado: Autor.

4.5.1.2.8 Políticas de redes

Propósito: Preservar y mantener los datos transmitidos sobre redes minimizando el riesgo generado por acceso indebido a las mismas, logrando proporcionar un tráfico seguro de datos de una Pyme.

Acciones:

- Los datos transmitidos sobre redes públicas deben ser encriptados.
- El acceso a redes externas (públicas y privadas) debe hacerse a través de un firewall.
- Se debe identificar y autenticar cualquier sujeto en la red institucional.
- Sólo se permiten habilitar los siguientes servicios de red: SMTP, POP3, HTTP, SSH, SFTP, HTTPS.
- Se debe etiquetar en forma externa las redes disponibles como de acceso abierto, acceso restringido o acceso altamente restringido, de modo que los usuarios o propietarios de los datos estén al tanto de la protección ofrecida.
- Un responsable del área de Sistemas deberá gestionar el acceso a los servicios y recursos de red, de acuerdo a las responsabilidades de cada cargo o por solicitud formal de un empleado aprobado por el Jefe de Área respectivo.

- El camino de las comunicaciones será controlado, es decir se limitarán las opciones de elección de la ruta entre la terminal de usuario y los servicios a los cuales el mismo se encuentra autorizado a acceder, mediante la implementación de controles en diferentes puntos de la misma. Dichos controles se podrán implementar en los gateways que separan los diferentes dominios de la red.
- Se incorporarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen la Política de Control de Accesos. Estos controles contemplarán mínimamente la verificación positiva de direcciones de origen y destino.
- La configuración de enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red; debe ser documentada, y mantenida por el responsable del Área de Sistemas respectivo.

Tabla 4.6 Políticas de Redes

Elaborado: Autor.

4.5.1.2.9 Políticas de correo electrónico

Propósito: Asegurar la privacidad de los mensajes de correo electrónico, el buen uso de los mismos y el compromiso inherente entre la Pyme y sus miembros respecto a este servicio.

Acciones:

- Para las operaciones, únicamente se utilizarán los correos electrónicos asignados por la Pyme, no se puede emplear direcciones de correo electrónico diferentes a las cuentas oficiales para atender asuntos de trabajo.
- La información general puede enviarse dentro de la Pyme sin encriptación, pero la información confidencial siempre debe ser encriptada. Todos los mensajes de correo electrónico que contengan información concerniente, a números de tarjetas de crédito, claves de acceso, información de investigación y desarrollo e información sensible de entidades externas, debe ser encriptados antes de ser

transmitidos.

- Todos los mensajes de correo electrónico deben contener el nombre y apellidos del remitente, su cargo, dirección y número telefónico.
- En todos los mensajes de correo electrónico salientes, debe agregarse un pie de página, en el que se indique que el mensaje puede contener información confidencial, que es para el uso de los destinatarios nombrados, que ha sido registrado para propósitos de archivo.
- El personal no debe abrir archivos adjuntos de correos electrónicos desconocidos, a menos que hayan sido descargados y analizados por el software antivirus aprobado.
- Queda prohibido acceder a mensajes de correo electrónico tipo SPAM, así como también retransmitir este tipo de mensajes.
- No está autorizado enviar mensajes que contengan virus, datos corruptos, texto acosador, difamatorio, obsceno, que atente contra la integridad del personal y/o de la empresa.
- El tamaño permitido de archivos adjuntos no debe exceder de 10MB en un correo electrónico.
- El correo electrónico no debe ser considerado como medio de almacenamiento, por lo que el usuario deberá realizar un mantenimiento constante de su cuenta, archivando la información importante, eliminando correos, etc.
- El responsable de IT deberá monitorizar el uso de correo electrónico del personal, así como también asegurar la eliminación constante de correos con histórico mayor a tres meses.

Tabla 4.7 Políticas de Correo electrónico.

Elaborado: Autor.

4.5.1.2.10 Políticas de comercio electrónico

Propósito: Prevenir la revelación de información privada, fraude, o violación a la privacidad de la información de cuentas y la seguridad de las transacciones realizadas a través de Internet o redes externas.
Acciones: • Toda información acerca de pagos, como números de cuentas corrientes y de tarjetas de crédito, debe ser encriptada mientras esté almacenada en computadores accesibles desde Internet o desde redes externas. • Se tomarán recaudos para la protección de la integridad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada. • Todos las transacciones realizadas a través de la página web de la Pyme deben ser documentadas y archivadas, máximo hasta las siguientes dos semanas a partir de su ejecución. • Se debe establecer de manera clara una política de seguridad del sitio, para que el usuario conozca el manejo de la información. • La información personal del cliente, solo puede ser utilizada para enviar promociones, servicios. No puede ser compartida para otro tipo de actividad. • Establecer procesos de entrega de productos y/o servicios. • Definir procedimientos de reembolso, quejas y devoluciones.

Tabla 4.8 Políticas de Comercio electrónico.

Elaborado: Autor.

4.5.1.2.11 Políticas de Internet

Propósito: Formular controles que permitan minimizar el riesgo generado por el acceso a Internet, el cual expone directamente a la Pyme con código malicioso o nocivo, el cual puede comprometer directamente la integridad, la disponibilidad y la confidencialidad de

la información procesada por cada uno de los componentes de la red.
Acciones: • Tendrán acceso al Internet personal administrativo, y para este caso, los responsables del comercio electrónico en la Pyme. • Los navegadores permitidos deberán establecerse de acuerdo a requerimientos para uso de la web de la Pyme. Las opciones son: Internet Explorer, Mozilla Firefox, y Google Chrome. • No se debe utilizar el Internet para visualizar o descargar música, películas u otros archivos no legales; material pornográfico; descargar software peligroso, no licenciado, o de contenido ilícito; o para uso privado, etc. • No se deben abrir documentos adjuntos o hacer clic en enlaces de mensajes no solicitados o sospechosos. • Los usuarios deben abstenerse de visitar sitios restringidos por la institución de manera explícita o implícita, o sitios que afecten la productividad de la Pyme. • Además, no deben brindar cualquier tipo de información institucional en sitios no autorizados o que no cuenten con mecanismos de seguridad que garanticen la confidencialidad de la información en tránsito. • Tampoco se debe utilizar el Internet para participar en grupos de discusión en Internet, Listas de Correo, chats o cualquier otro foro público, a menos que su participación haya sido expresamente autorizada formalmente por la Pyme. • El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto. • El responsable del área de Sistemas, deberá definir procedimientos eficaces para solicitar y aprobar accesos a Internet. Los accesos serán autorizados por el Jefe de Área respectivo.

Tabla 4.9Políticas de Internet.

Elaborado: Autor.

4.5.1.2.12 Políticas de firewall

Propósito: Las políticas de firewall o cortafuegos permiten bloquear o permitir determinados tipos de tráfico de red no especificados la política de excepciones de Internet.
Acciones: • Los equipos de firewall deben estar sujetos a un monitoreo regular y a una auditoria anual. • Las conexiones de los usuarios que accedan desde el Internet deben usar un sistema de autenticación robusto. • Todos los accesos al Internet desde la red de la institución deben hacerse sobre proxys localizadas en un firewall.

Tabla 4.10Políticas de Control de firewall.

Elaborado: Autor.

4.5.1.2.13 Políticas de backup

Propósito: Proporcionar lineamientos que ayuden a mantener la disponibilidad de la información de acuerdo a las necesidades de continuidad planeadas a nivel de los procesos y por ende de la Pyme.
Acciones: • Definir el mecanismo y/o programa para realizar respaldos de información. • El usuario deberá depurar la información previo a realizar un respaldo. • Debe existir un responsable del área de Sistemas que realice los respaldos y la restauración de los mismos. Solo el encargado puede realizar dichas tareas. • Los respaldos deben hacerse con regularidad en base a un cronograma

preestablecido, se recomienda sean realizados con una frecuencia diaria.

- Realizar la clasificación de información: frecuente, debe ser información liviana para acceso rápido; histórica, es robusta y pesada, se acceda de manera esporádica a esta información y el respaldo puede ser a un lapso mayor al definido para la información frecuente.
- Se deben documentar los procedimientos para restaurar el sistema después de fallas serias en los discos u otros componentes de hardware y bajo diferentes tipos de desastres.
- Será necesario identificar mecanismos que permitan que las actividades de respaldo y recuperación de la información sean las más adecuadas, en lo relativo a costo / beneficio.
- Establecer procedimiento para sincronización de información vs. backups.
- El responsable de los backups deberá definir procedimientos adecuados para la eliminación segura de los medios de información respetando el cuidado del medio ambiente
- Determinar la ubicación y seguridad donde se colocarán los respaldos.

Tabla 4.11Políticas de Backups.

Elaborado: Autor.

4.5.1.3 Identificación de Activos y sus riesgos

4.5.1.3.1 Activos

Con el fin de identificar los activos y posibles factores de riesgo, es indispensable realizar un listado de los activos, el cual debe incluir tanto a los

activos tangibles (Hardware) como a los intangibles (Software e Información) participes en el comercio electrónico.

Cada uno de los activos deben estar identificados, la ISO clasifica a los activos de la siguiente manera:

- Activos de Información: Son las bases de datos y archivos de datos, documentación del sistema, manuales de usuario, material de entrenamiento, procedimiento de operativos de apoyo, planes de continuidad más.
- Documentos Impresos: Lineamientos, documentos de la institución, documentos que contengan información importante del negocio.
- Activos de Software: Software de aplicación, software de sistemas, herramientas de desarrollo, etc.
- Activos Físicos: Equipos de comunicación y computación, medios de almacenamiento, otros equipos técnicos.
- Personas: Personal, clientes y suscriptores.
- Empresa: Imagen y Reputación de la Compañía.
- Servicios: Servicios de computación y comunicaciones, demás servicios técnicos.

A dichos activos se les deberá asignar la importancia que tienen para la Pyme y para el proceso de comercio electrónico como tal. Dichos activos deberán ser calificados con una escala de 1 al 10, donde 1 es menor importancia y 10 es

la mayor; este valor reflejará el nivel de impacto que puede tener en la Pyme si un incidente (falta o falla del mismo)lo afecta.

Para esto se utilizará el siguiente formato:

N°	Nombre	Características	Valor (USD)	Nivel de Importancia (1 -10)
1				
2				
… n				

Tabla 4.12 Formato Activos.

Elaborado: Autor.

4.5.1.3.2 Factores de riesgo

Asimismo, se deberán definir los factores de riesgo más importantes a los que pueden verse expuestos cada uno de los activos anteriormente identificados; además, se deberá indicar la probabilidad de que estos ocurran y la afectación de los mismos a las actividades de la empresa. Para esto, se considerará una escala entre 1 y 3, donde 1 es menor y 3 es mayor.

Entre los más destacados, se tienen:

N°	Factores de Riesgo	Probabilidad de acontecimiento	Ponderación de afectación
1	Acceso no autorizado a las instalaciones	1	2
2	Acceso no autorizado a los datos	1	3
3	Afectación en la integridad de los datos	2	3
4	Cracking de claves	2	3
5	Daño de los equipos y/o redes	1	2
6	Daños/Pérdida de los backups	2	2
7	Desabastecimiento de energía o variaciones de voltaje	3	2
8	Desastres naturales	1	2
9	Errores de software	2	2
10	Errores en la encriptación de datos	1	3
11	Falla en los servicios web	3	2
12	Fallas de las BDD	1	3
13	Fallas del sistema	2	3
14	Usurpación de usuarios	2	3
15	Virus/Spam	3	3
… n			

Tabla 4.13 Formato Factores de riesgo.

Elaborado: Autor.

Se recomienda considerar todos los factores de riesgo arriba mencionados, pero si solo se tomará en cuenta algunos de estos, es importante seleccionar los de mayor valor de afectación.

4.5.1.3.3 Consecuencias

Posteriormente, se deberá elaborar una descripción de las consecuencias que podrían perjudicar al comercio electrónico de una Pyme si los activos son afectados por sus respectivos factores de riesgo.

Además, se deberá detallar como se protege actualmente el activo contra un factor en particular, y puntualizando el grado de efectividad de dichas medidas.

Para esto, se listarán los activos, los factores de riesgos que los afectan, las consecuencias, la protección actual y la efectividad de la misma (Baja, Media o Alta).

Activo	Factor de Riesgo	Consecuencias	Medidas	Efectividad (Baja, Media o Alta)
1	1			
	2			
	… n			
2	1			
	2			

	...n			
...n	1			
	2			
	...n			

Tabla 4.14Formato Consecuencias y Medidas.

Elaborado: Autor.

4.5.1.3.4 Vulnerabilidad

En base a lo anteriormente mencionado, se procederá con el cálculo de niveles de vulnerabilidad asociados a cada activo. Para esto, se deberán realizar las siguientes operaciones:

- Probabilidad del Riesgo: Porcentaje de que ocurra un determinado factor de riesgo, con respecto a la cantidad de factores de riesgo relacionados a dicho activo.
- Nivel de Vulnerabilidad: Nivel de importancia multiplicado por la probabilidad del riesgo. De esta forma, se obtiene el nivel de vulnerabilidad de cada activo con respecto a un factor de riesgo. La suma de estos valores es el nivel de vulnerabilidad total que corresponde a cada activo.

Activo	Nivel de importancia	Probabilidad de acontecimiento	Probabilidad de riesgo	Nivel de vulnerabilidad
1				
2				
... n				

Tabla 4.15Formato Vulnerabilidad.

Elaborado: Autor.

4.5.1.4 Control de Riesgos

Considerando los resultados obtenidos, se procederá con la evaluación de la situación actual de los activos considerados en el comercio electrónico de una Pyme, en relación a los acontecimientos que pueden malograrlos.

El análisis de riesgos realizado ayudará a determinar cuáles son los activos que tienen mayor vulnerabilidad ante factores externos o internos que puedan perjudicarlos, identificando las causas que faciliten o imposibiliten alcanzar los objetivos, y considerando el grado en que el riesgo pueda ser controlado.

Es así, que después de haber identificado y cuantificado los riesgos, se deben determinar los objetivos y los procedimientos de control respectivos.

4.5.1.5 Fijación de controles y objetivos de control

Una vez propuestas las diferentes políticas a aplicar y de evaluar los riesgos a los cuales están expuestos los activos de una Pyme, los objetivos de control se resumen en los siguientes:

- Asegurar la confiabilidad de datos manejados en el proceso de eCommerce.
- Fortalecer la constante disponibilidad de información para el efectivo comercio electrónico de una Pyme.
- Garantizar la integridad de la información participe de este proceso.

A continuación, se presenta una serie de controles frecuentes a implementar. En este punto, cabe acotar que los controles dependerán de la evaluación de riesgos anteriormente realizada, pero para este caso, se proponen controles básicos necesarios para el correcto funcionamiento del comercio electrónico en una Pyme.

N°	Control	Ejecución	Garantías
1	**Inventario de activos**	Todos los activos deberán estar claramente identificados, manteniendo un registro de los mismos.	No descartar ningún activo y validar su existencia constantemente. Documento de respaldo: Kárdex de activos tangibles e intangibles de la Pyme.
2	**Responsables de los activos**	Todos los activos deberán ser asignados a un responsable.	El responsable puede tomar las decisiones necesarias relativas a la información bajo su control a fin de mantener integridad y confidencialidad Documentos de respaldo: Manual de procedimiento para entrega de responsabilidades de activos y Actas de entrega-recepción de activos.
3	**Funciones y responsabilidades del Personal**	Se deberá definir y documentar los roles y responsabilidades de la seguridad de los empleados, en correspondencia con la política de seguridad de la información de la Pyme.	Establecer responsabilidades en base a jerarquías de trabajo Documento de respaldo: Manual de responsabilidades y seguridad en el cumplimiento de su función.

4	**Sanciones disciplinarias**	Deberá haber un proceso formal disciplinario para el personal que produzca brechas en la seguridad de la información.	Aplicar las sanciones correctoras necesarias. Documento de respaldo: Manual de sanciones.
5	**Seguridad física**	Las herramientas de seguridad como cámaras IP, tarjetas de control de entrada a puertas, etc. deberán utilizarse para proteger las áreas que contengan información confidencial.	Contar con la seguridad física necesaria acorde a la importancia de la información. Documento de respaldo: Manual de controles a áreas restringidas.
6	**Amenazas humanas y desastres naturales**	Se deberá designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión u otras formas de desastre natural o humano.	Asegurar la información con diferentes tipos de protección para garantizar su seguridad. Documento de respaldo: Manual y plan de contingencia contra las amenazas naturales o humanas.
7	**Protección de equipos**	Los equipos deberán ser ubicados en lugar de difícil acceso y así evitar que sean manipulados por personas no autorizadas.	Evitar el acceso no autorizado tomando las debidas precauciones en base a la ubicación de los equipos. Documento de respaldo: Manual y plan de contingencia contra las amenazas naturales o humanas.

8	**Seguridad del cableado**	Se deberá proteger el cableado que transporten datos o que soporten servicios de información contra posibles interceptaciones o daños.	Etiquetar el cableado y evitar los cableados sueltos o dispersos, estos deberán entubarse. Documento de respaldo: Manual de redes.
9	**Gestión de cambios**	Se deberán controlar los cambios en los sistemas, en las BDD y en los recursos de tratamiento de la información.	Registrar todo tipo de modificación y limitar los cambios. Documento de respaldo: Manual de procedimiento de Gestión de Cambios.
10	**Suministro de servicios**	Se deberá garantizar que los controles de seguridad y entrega sean implementados y mantenidos por los proveedores.	Asignar las responsabilidades para el manejo de este tipo de situaciones. Documento de respaldo: Reportes mensuales sobre la provisión de servicios.
11	**Controles contra el código malicioso**	Se deberá implantar controles de detección, prevención y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de los usuarios.	El personal deberá encargarse de detectar y eliminar la infección o contagio de código malicioso. Documento de respaldo: Manual de controles contra el software malicioso y concienciación de los usuarios.

12	**Backups**	Se deberán hacer regularmente backups de toda la información esencial del negocio.	Hacer copias permanentes de seguridad con periodos de tiempo de acuerdo a la importancia de la información. Documento de respaldo: Manual para backups.
13	**Controles de red**	Se deberá mantener y controlar adecuadamente las redes para protegerlas de amenazas.	Evitar el acceso de usuarios no autorizados Documento de respaldo: Manual de redes.
14	**Administración de la información**	Se deberá establecer procedimientos para la manipulación y almacenamiento de la información	Cuidar su información contra divulgaciones o usos inadecuados. Documento de respaldo: Manual de administración de la información.
15	**Mensajería electrónica**	Se deberá proteger adecuadamente la información contenida en la mensajería electrónica.	Proteger la información enviada o recibida en los emails. Documento de respaldo: Manual de Seguridad de Mensajería Electrónica.
16	**Sistemas de información**	Se deberá desarrollar e implementar procedimientos con el fin de proteger la información asociada con la interconexión de sistemas de información del	Revisar la seguridad de los sistemas de información periódicamente. Documento de respaldo: Política de seguridad en la interconexión de sistemas de

		negocio.	información del negocio.
17	**Comercio electrónico**	Se deberá proteger la información involucrada en el comercio electrónico contra actividades fraudulentas.	Garantizar la seguridad del uso de redes públicas para evitar pérdidas considerables de la información. Documento de respaldo: Manual de comercio electrónico.
18	**Actividades comerciales en línea**	Se deberá proteger la información implicada en las transacciones en línea para prevenir la transmisión incompleta o alteración no autorizada de la información.	Garantizar la seguridad de las transacciones comerciales en línea. Documento de respaldo: Manual de comercio electrónico.
19	**Información pública**	Se deberá proteger la integridad de la información que se pone a disposición en un sistema de acceso público para prevenir modificaciones no autorizadas.	Se debe evitar la manipulación no autorizada de la información con medidas puntuales de la integridad de la información. Documento de respaldo: Política de acceso público a los sistemas de información.
20	**Uso del sistema**	Se deberán establecer procedimientos para el uso del monitoreo del uso de los sistemas.	Revisar los resultados de las actividades de monitoreo, para establecer los procedimientos

			adecuados para su correcto uso. Documentos de respaldo: Manual para el monitoreo de uso de los sistema e Informe de Supervisión.
21	**Control de acceso**	Se deberá establecer una gestión de usuarios y contraseñas, así como el control de accesos de los mismos.	Restringir y administrar el acceso. Documento de respaldo: Manual de gestión de usuarios y restricción de accesos.
22	**Privilegios**	Se deberá controlar la asignación y uso de los privilegios.	Registrar el cambio en los roles y responsabilidades de los usuarios y gestionar de acuerdo a su nueva realidad los privilegios de acceso. Documento de respaldo: Manual de gestión de usuarios y restricción de accesos.
23	**Acceso a la red**	Se deberá proveer a los usuarios los accesos a los servicios para los que han sido autorizados.	Contar con las garantías de acceso a la red y ejecutar el control de las conexiones, considerando jerarquías de autorización de acceso. Documento de respaldo: Manual de uso de los servicios de Red.

26	**Acceso a la información**	Se deberá restringir el acceso de los usuarios a la información y funciones de los sistemas de aplicaciones.	Controlar, asegurar y establecer prioridades de acceso autorizado a la información. Documento de respaldo: Manual de gestión de usuarios y restricción de accesos.
27	**Controles criptográficos.**	Se deberá desarrollar e implantar el uso de controles criptográficos para la protección de la información.	Contar con controles criptográficos para el tratamiento de la información. Documento de respaldo: Manual de controles criptográficos.
28	**Administración de claves**	Se deberá establecer una administración de las claves que respalde el uso de las técnicas criptográficas.	Asignar claves basadas en técnicas criptográficas. Documento de respaldo: Manual de controles criptográficos.
29	**Control de vulnerabilidades**	Se deberá analizar los sistemas de información y a qué tipo de vulnerabilidades están expuestas, evaluar la amenaza y tomar las medidas adecuadas para minimizar los riesgos	Realizar una capacitación al personal sobre las vulnerabilidades de los sistemas de información que se están utilizando y así evitar el perjuicio o daños de los mismos. Documento de respaldo: Manual de gestión de vulnerabilidades.

30	**Continuidad del negocio**	Se deberán desarrollar e implantar planes de mantenimiento o recuperación de las operaciones del proceso de comercio electrónico, para asegurar la disponibilidad de la información, tras una interrupción o fallo técnico.	Desarrollar un plan de contingencia que establezca y organice los riesgos, responsabilidades y procedimientos a seguir. Documento de respaldo: Manual y Plan de continuidad.

Tabla 4.16 Controles.

Elaborado: Autor.

4.5.1.6 Definición de la Declaración de la Aplicabilidad

Al considerar los riesgos con mayor peso, se propone una serie de controles que mitigarán sus efectos en el comercio electrónico de una Pyme. Estos se basan en los diferentes tipos de políticas enunciadas en el apartado 4.5.2, considerando los factores de riesgos mencionados.

Es importante acotar que dichos controles son los propuestos o sugeridos en este proyecto, pero para una mayor personalización las pequeñas y medianas empresas deberán desarrollar un SGSI acorde a su realidad.

Para esto, las Pymes deberán tomar la metodología aquí diseñada y ejecutarla paso a paso, de esta manera, se logrará aplicar un control efectivo de la seguridad de la información, basado en la ISO 27001.

4.5.2 Fase de Implementación

En la fase de implementación del SGSI en una Pyme ecuatoriana, son varios aspectos que se deben considerar, entre estos se destacan:

- Selección del personal involucrado
- Adaptación del SGSI
- Documentación del SGSI
- Cronograma de aplicación
- Capacitación de la nueva metodología adoptada

1. Selección del personal involucrado	Definición de los responsables del proceso y de las responsabilidades de los mismos.	▪ Gerente ▪ Jefes de Área ▪ Personal del Área de Sistema	Primer trimestre del año
2. Adaptación del SGSI	En base a esta propuesta y a la realidad	▪ Jefes de Área	Primer trimestre del

	de cada Pyme, la empresa en cuestión debe adaptar la implementación de acuerdo a sus necesidades y recursos.	▪ Personal del Área de Sistema ▪ Experto contratado (si fuera el caso)	año
3. Documentación del SGSI	Crear un manual personalizado sobre el SGSI propio de la Pyme.	▪ Personal del Área de Sistema ▪ Experto contratado (si fuera el caso)	Segundo trimestre del año
4. Cronograma de aplicación	Tiempo exacto de ejecución de las actividades sobre implementación, verificación, mantenimiento y mejora.	▪ Jefes de Área ▪ Personal del Área de Sistema ▪ Experto contratado (si fuera el caso)	Segundo trimestre del año
5. Capacitación de la nueva metodología adoptada	Difusión y capacitación sobre el "Sistema de gestión de la seguridad de la información para comercio electrónico" implementado en la Pyme.	▪ Jefes de Área ▪ Personal del Área de Sistema ▪ Experto contratado (si fuera el caso)	Tercer trimestre del año

Tabla 4.17 Implementación del SGSI.

Elaborado: Autor.

4.5.3 Fase de Verificación

Para esta fase se determinan dos aspectos importantes a ejecutar, estos son:

- Revisiones periódicas
- Auditorías al SGSI implantado.

1. Comprobación de Aplicabilidad	Comprobación de la real aplicabilidad del SGSI en la Pyme.	▪ Personal del Área de Sistema ▪ Experto contratado (si fuera el caso) ▪ Responsables de los activos de información	Tercer trimestre del año
2. Comprobación del cumplimiento	Comprobación del cumplimiento de las normas y procedimientos de seguridad establecidos, mediante revisiones periódicas.	▪ Jefes de Área ▪ Personal del Área de Sistema	Una vez cada trimestre del año.
3. Auditoria del SGSI	Planificación y ejecución de	▪ Jefes de Área	Una vez al año, cuarto

	actividades de auditoría que impliquen comprobaciones en los sistemas en activo.	▪ Personal del Área de Sistema ▪ Experto contratado (si fuera el caso) ▪ Responsables de los activos de información	trimestre.

Tabla 4.18Verificación del SGSI.

Elaborado: Autor.

4.5.4 Fase de Mantenimiento y mejora

Finalmente, para la fase de mantenimiento y mejora se identifican los siguientes aspectos claves a establecer:

- Planes de continuidad de las actividades
- Acciones correctivas o nuevas políticas

Elaboración y aplicación de los Planes de Continuidad de las Actividades	Elaboración de planes de contingencia efectivos y necesarios para garantizar la continuidad de las actividades.	▪ Jefes de Área ▪ Personal del Área de Sistema	Cuarto trimestre del año
Mantenimiento y reevaluación de los Planes de Continuidad de la Pyme	Se establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.	▪ Personal del Área de Sistema ▪ Experto contratado (si fuera el caso)	Una vez al año
Ejecución de Acciones correctivas o nuevas políticas	En base a los resultados de la verificación del SGSI, se deben ejecutar acciones correctivas o implementar nuevas políticas, según sea el caso.	▪ Jefes de Área ▪ Personal del Área de Sistema	Una vez cada trimestre del año

Tabla 4.19Mantenimiento y mejora del SGSI.

Elaborado: Autor.

CONCLUSIONES

Una vez realizada la investigación, recolección de información y análisis de datos, se obtuvo resultados que presentan las siguientes conclusiones:

- A lo largo de mi experiencia laboral tanto en empresas privadas, como en el sector público, he podido observar el deficiente interés que tiene la Dirección y/o Gerencia respecto a manejar políticas que ayuden a mantener un adecuado SGSI, esto a su vez ocasiona que la mayoría del personal de IT pierda el objetivo de la responsabilidad que tienen sobre los activos tecnológicos y el control de la información.

- Hoy en día las PYMES en Ecuador contribuyen de manera importante a la generación de empleo mediante la producción de bienes y servicios, la mayoría de Pymes requieren incursionar en al ámbito del comercio electrónico debido a la globalización, por eso la importancia de manejar un adecuado sistema de Gestión para la Seguridad de la Información, ya que es imperante minimizar riesgos del activo más importante. Sin embargo, son pocas las Pymes que invierten en recursos para salvaguardar la información, ya que una característica común de este tipo de negocios es el insuficiente financiamiento que tienen versus todas las

necesidades como inversión en maquinaria para fabricación de productos, materia prima, personal, etc.

- Adicionalmente, en Ecuador todavía no existe una cultura organizacional para prevenir incidentes que afecten a la seguridad de la información, el compromiso de la Dirección y/o Gerencia General mantiene su visión apegada al comercio, mercadeo, etc., dejando las necesidades informáticas al final de la lista. La decisión de aplicar estándares internacionales de calidad como la norma ISO 27001 en la Pymes no necesariamente lo plantea la Dirección y/o Gerencia General. Por ello, es importante contar con personal competente que este alineado al cumplimiento de los objetivos organizacionales, es así, que el responsable del área informática debe trabajar enfocado a mantener un adecuado SGSI, y para lograr esto, debe realizar todos los análisis necesarios para evaluar el impacto en caso de poner en riesgo la información, así como también, las pérdidas económicas que pueden generarse, proponiendo mecanismos y planes de acción específicos para captar la atención y el compromiso de las autoridades, y de esta manera aprueben implantar un SGSI basado en la norma ISO 27001, garantizando que así tengan recursos limitados las inversiones sean bien enfocadas.

- En el manejo de comercio electrónico los riesgos aumentan día a día de manera significativa, por tal razón establecer un Sistema de Gestión de

Seguridad de la Información basado en la Norma ISO 27001 se convierte en una herramienta de control idónea para las Pymes Ecuatorianas, ya que permitirá de una manera sistemática administrar y salvaguardar la información sensible de la compañía, para que permanezca protegida, evaluando permanente las metodologías, los controles, procesos, etc., lo cual fortalecerá la seguridad, disponibilidad, el acceso, el control, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, frente a posibles hackeos, y de esta manera permitir a la organización cumplir con sus objetivos institucionales, implementando sistemas que tengan un especial cuidado con la información.

- Independientemente de que la norma 27001 proponga una serie de documentos estándar para tomar medidas preventivas y reactivas para resguardar y proteger la información, es la propia organización la que decide cómo manejar la seguridad de la información y que métricas desea implementar, en base a lo que considera que es importante medir o evaluar. Sin el compromiso sobre todo de la Alta Dirección y/o Gerencia General, cualquier sistema de seguridad es vulnerable.

- Es importante tener en cuenta que la mayor dificultad de los SGSI se encuentra en cómo medir su eficacia y eficiencia. No se ha desarrollado una forma totalmente cuantitativa para medir la seguridad de la información. Hay algunas aproximaciones, basadas en estimaciones subjetivas del personal informático y personal Gerencial. En general, se

consideran cuestiones como por ejemplo “entrenamiento del personal”, ítem al cual se le asigna un valor en las métricas tradicionales, cuando en realidad debe considerarse cuál es el valor del entrenamiento del personal para enfrentar cada posible peligro en particular.

- Una gran parte del éxito del SGSI se basa en proponer métricas de rendimiento de la seguridad de la información para obtener un valor que no solo determina el nivel de calidad y madurez de la seguridad, como los métodos tradicionales, sino que también que indica dónde y en qué orden realizar inversiones para mejorar el valor de la métrica y por consiguiente la seguridad de la información, asegurando la mejor relación costo-beneficio.

- La elaboración de esta disertación, contribuirá a las Pymes Ecuatorianas a la toma de conciencia sobre la importancia de la información, para que esta sea confiable, integra y disponible para la organización, adicionalmente es una guía que muestra las características de implantar un sistema de Gestión de la información basado en el cumplimiento de la norma ISO 27001.

RECOMENDACIONES

La experiencia recopilada en el trascurso del desarrollo de esta tesis me ha permitido encontrar puntos importantes para realizar las siguientes recomendaciones:

- Es fundamental orientar la implantación de una estructura de procesos dentro de la organización, entendiendo por proceso cualquier actividad que emplea recursos para permitir la transformación de entradas en salidas. Por lo que es necesario que la Dirección de Tecnología (IT) de la Pyme conjuntamente con la Alta Gerencia evalúen la importancia que tiene la información que se maneja dentro de la empresa, y se defina si las medidas de seguridad con las que cuentan actualmente son suficientes para la protección de la información. Muchas decisiones respecto al cumplimiento de políticas dentro SGSI deben ser de carácter jerárquico, impulsado por el director de la organización, siendo este el primer paso para adaptarse a todo cambio coyuntural dentro de la empresa.

- La concientización del personal de la compañía sobre la importancia de trabajar en un ambiente de procesos, es un pilar fundamental de toda norma de calidad, por lo cual las organizaciones deben ingeniosamente

buscar y adoptar mecanismos que permitan que se despierte un interés y compromiso por parte de todos los empleados.

- Las organizaciones deben tratar de hacer lo más llevadero posible las tareas operativas del sistema SGSI, para lo cual necesitan la ayuda de herramientas tecnológicas que automaticen ciertas tareas, específicamente para el análisis y Gestión de Riesgos se recomienda adquirir o implementar una herramienta.

- Es necesario tener claro que un SGSI no puede ser implantado por moda, el criterio de este, debe ser manejado con responsabilidad y siempre buscando objetivos claros que agreguen valor a la organización.

- Proporcionar al área de sistemas los recursos necesarios para mantener el SGSI en la empresa, así como también capacitar al personal del área para que sean agentes de toma de decisiones oportunas respecto a medidas de seguridad informática.

- Es necesario que dentro del Departamento de sistemas exista un grupo de personas, cuyas funciones sean las de administrar la seguridad de la información en la empresa.

- Establecer un plan de auditorías periódicas al SGSI de la PYME, para análisis de vulnerabilidades y determinar de manera oportuna los procedimientos a seguir para minimizar los riesgos.

- El personal encargado de la seguridad de la información deberá monitorear constantemente los factores de riesgos existentes en la organización, así como también el cumplimiento de los planes de acción definidos como resultado de las auditorías.

- Deberán crearse y actualizarse Políticas de seguridad en base a los resultados del análisis de riesgo y /o auditorías. Estas políticas deben ser claras para la correcta difusión, entendimiento y conocimiento de todo el personal.

- El sistema de gestión de la información necesita cumplir con un ciclo PDCA, por lo que se debe actualizar el Plan de Seguridad de Información con cada evaluación de riesgo de la empresa.

- La Gerencia deberá establecer sanciones para el personal que incumpla con las políticas de seguridad definidas dentro del SGSI.

- Se puede mencionar la ISO 27002 como una guía de buenas prácticas para la gestión de riesgos, que expone recomendaciones a tener en cuenta para cada uno de los controles de la ISO 27001.

BIBLIOGRAFÍA

ÁREA DE CIENCIAS DE LA COMPUTACIÓN E INTELIGENCIA ARTIFICIAL - Universidad de Vigo (s.f.). Estándares y Normas de Seguridad. Recuperado el 17 de Julio de 2013, de http://ccia.ei.uvigo.es/docencia/SSI/normas-leyes.pdf.

AREITIO, Javier (2008). Seguridad de la información: redes, informática y sistemas de información. Madrid, España: Editorial Paraninfo.

ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD (2013). La norma ISO 27001 del Sistema de Gestión de la Seguridad de la Información - Garantía de confidencialidad, integridad y disponibilidad de la información-. Recuperado el 17 de Julio de 2013, de http://www.aec.es/c/document_library/get_file?uuid=a89e72de-d92b-47cf-ba5e-5ea421fcbeb4&groupId=10128.

ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD (2013). Seguridad de la Información. Recuperado el 1 de Mayo de 2013, de http://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion.

ATEHORTÚA, F., BUSTAMANTE, R., VALENCIA, J. (2008). Sistema de gestión integral. Una sola gestión, un solo equipo. Medellín, Colombia: Universidad de Antioquia.

BSI (2012). Seguridad de la Información. Recuperado el 17 de Junio de 2013, de http://www.bsigroup.es/certificacion-y-auditoria/Sistemas-de-

gestion/estandares-esquemas/Seguridad-de-la-Informacion-ISOIEC27001/.

DEL PESO, Emilio (2003). Manual de outsourcing informático. Madrid, España: Ediciones Díaz de Santos.

GARCÍA A. & ALEGRE, M. (2011). Seguridad informática. Madrid, España: Paraninfo.

http://www.iso27000.es/iso27000.html#section3b.

IS & BCA, 2013. Conceptos básicos sobre ISO 27001. Recuperado el 17 de Junio de 2013, de http://www.iso27001standard.com/es/que-es-la-norma-iso-27001.

ISO (s.f.a). About ISO. Recuperado el 10 de Junio de 2013, de http://www.iso.org/iso/home/about.htm

ISO (s.f.b). Standards Development. Recuperado el 10 de Junio de 2013, de http://www.iso.org/iso/home/standards_development.htm.

ISO27000 (2012a). Origen. Recuperado el 12 de Junio de 2013, de http://www.iso27000.es/iso27000.html#section3a.

ISO27000 (2012b). ISO 27000. Recuperado el 12 de Junio de 2013, de http://www.iso27000.es/iso27000.html.

ISO27000 (2012c). Serie 27000. Recuperado el 12 de Junio de 2013, de

ISO27000 (2012d). Beneficios. Recuperado el 14 de Junio de 2013, de http://www.iso27000.es/iso27000.html#section3d

ISO27000 (2012d). Contenido. Recuperado el 14 de Junio de 2013, de http://www.iso27000.es/iso27000.html#section3c.

ISO27000 (2012e). SGSI. Recuperado el 17 de Junio de 2013, de http://www.iso27000.es/sgsi.html.

PROGRAMA PARA EL DESARROLLO DEL COMERCIO ELECTRÓNICO EN LA COMUNIDAD DE MADRID (s.f.). Guía Práctica de Comercio Electrónico para Pymes. Recuperado el 15 de Julio de 2013, de http://ecommerce.madrid.org/attachments/article/3/Guia%20PYMES%20completa.pdf.

SEGURIDAD PARA TODOS (2013). ¿Seguridad Informática o Seguridad de la Información?. Recuperado el 1 de Mayo de 2013, de http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html.

SRI (2010). Pymes. Recuperado el 15 de Julio de 2013, de http://www.sri.gob.ec/web/10138/32@public.

TÜV SÜD IBERIA (s.f.). ISO/IEC 27001 - Sistema de Gestión de Seguridad de la Información. Recuperado el 17 de Julio de 2013, de http://www.tuv-sud.es/uploads/images/1350635458019372390409/pdf2-0039-iso-iec-27001-es-260412.pdf.

ANEXOS

ANEXO 1: MARCO CONCEPTUAL

- Amenaza: Cualquier evento que pueda provocar daño a la información.
- Hackeo: (Hackear) Acción que realiza un Hacker, para esto caso, persona que viola las seguridades de la información.
- Información: Conjunto de datos que se gestiona dentro de una organización.
- ISO: International Organization for Standardization - Organización Internacional de Normalización
- IEC: International Electrotechnical Commission - Comisión Electrotécnica Internacional.
- Pyme: (Pequeña y mediana empresa) es una empresa con características distintivas, y tiene dimensiones con ciertos límites ocupacionales y financieros prefijados por los Estados o regiones
- Riesgo: Probabilidad de que una amenaza se materialice sobre una vulnerabilidad del Sistema Informático, causando un impacto en la empresa.
- Seguridad de Información: Conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza.

- Seguridad Física: Protección del sistema ante las amenazas físicas, incendios, inundaciones, edificios, cables, control de accesos de personas, etc.
- Seguridad Informática: Conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza, se trata de un proceso en el cual participan personas.
- Seguridad Lógica: Protección de la información en su propio medio, mediante el enmascaramiento de la misma usando técnicas de criptografía.
- Sistema de Gestión de la Seguridad Informática (SGSI): Sistema de gestión que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información.
- Spam: Mensaje no solicitado, habitualmente de tipo publicitario, enviado en forma masiva a través del correo electrónico, puede presentarse por programas de mensajería instantánea o por teléfono celular.
- Vulnerabilidad: Cualquier debilidad que pueda permitir a las amenazas causar daño a los Sistemas y por ende a la Información.

ANEXO 2: ISO/IEC 270001:2005

ESTÁNDAR INTERNACIONAL

ISO/IEC 27001

Primera Edicion
2005 - 10 - 15

Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos

Numero de Referencia
ISO/IEC 27001:2005 (E)

SOLO PARA FINES DIDACTICOS

Tabla de Contenido

Prefacio 4
0 Introducción 5
0.1 General 5
0.2 Enfoque del Proceso 5
Figura 1 – Modelo PDCA aplicado a los procesos SGSI 6
0.3 Compatibilidad con otros sistemas de gestión 7
Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos 8
1 Alcance 8
1.1 General 8
1.2 Aplicación 8
2 Referencias normativas 9
3 Términos y definiciones 9
4 Sistema de gestión de seguridad de la información 12
4.1 Requerimientos generales 12
4.2 Establecer y manejar el SGSI 12
4.2.1 Establecer el SGSI 12
4.2.2 Implementar y operar el SGSI 14
4.2.3 Monitorear y revisar el SGSI 15
4.2.4 Mantener y mejorar el SGSI 16
4.3 Requerimientos de documentación 16
4.3.1 General 16
4.3.2 Control de documentos 17
4.3.3 Control de registros 17
5 Responsabilidad de la gerencia 18
5.1 Compromiso de la gerencia 18
5.2 Gestión de recursos 18
5.2.1 Provisión de recursos 18
5.2.2 Capacitación, conocimiento y capacidad 19
6 Auditorías internas SGSI 19
7 Revisión Gerencial del SGSI 20

SOLO PARA FINES DIDACTICOS

7.1 General 20
7.2 Insumo de la revisión 20
7.3 Resultado de la revisión 21
8 Mejoramiento del SGSI 21
8.1 Mejoramiento continuo 21
8.2 Acción correctiva 21
8.3 Acción preventiva 22
Anexo A 23
(normativo) 23
Objetivos de control y controles 23
Anexo B 37
(informativo) 37
Principios OECD y este Estándar Internacional 37
Tabla B.1 – Principios OECD y el modelo PDCA 37
Anexo C 39
(informativo) 39
Correspondencia entre ISO 9001:2000, ISO 14001:2004 y este Estándar Internacional 39
Tabla C.1 – Correspondencia entre ISO 9001:2000, ISO 14001:2004 y este Estándar Internacional 39
Bibliografía 40

SOLO PARA FINES DIDACTICOS

Prefacio

ISO (la Organización Internacional para la Estandarización) e IEC (la Comisión Electrotécnica Internacional) forman el sistema especializado para la estandarización universal. Los organismos nacionales miembros de ISO o IEC participan en el desarrollo de Estándares Internacionales a través de comités técnicos establecidos por la organización respectiva para lidiar con campos particulares de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no-gubernamentales, junto con ISO e IEC, también toman parte en el trabajo. En el campo de la tecnología de la información, ISO e IEC han establecido u comité técnico conjunto, ISO/IEC JTC 1.

Los Estándares Internacionales son desarrollados en concordancia con las reglas dadas en las Directivas ISO/IEC, Parte 2.

La tarea principal del comité técnico conjunto es preparar Estándares Internacionales. Los anteproyectos de los Estándares Internacionales adoptados por el comité técnico conjunto con enviados a los organismos nacionales para su votación. La publicación de un Estándar Internacional requiere la aprobación de por lo menos 75% de los organismos nacionales que emiten un voto.

Se debe prestar atención a la posibilidad que algunos elementos de este documento estén sujetos a derechos de patente. ISO e IEC no deben ser responsables de la identificación de algún o todos los derechos de patentes.

ISO/IEC 27001 fue preparado por el Comité Técnico Conjunto ISO/IEC JTC 1, Tecnología de la información, Subcomité SC 27, Técnicas de seguridad TI.

SOLO PARA FINES DIDACTICOS

0 Introducción

0.1 General

Este Estándar Internacional ha sido preparado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). La adopción de un SGSI debe ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que estos y sus sistemas de apoyo cambien a lo largo del tiempo. Se espera que la implementación de un SGSI se extienda en concordancia con las necesidades de la organización; por ejemplo, una situación simple requiere una solución SGSI simple.

Este Estándar Internacional puede ser utilizado por entidades internas y externas para evaluar la conformidad.

0.2 Enfoque del Proceso

Este Estándar Internacional promueve la adopción de un enfoque del proceso para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de una organización.

Una organización necesita identificar y manejar muchas actividades para poder funcionar de manera efectiva. Cualquier actividad que usa recursos y es manejada para permitir la transformación de Insumos en outputs, se puede considerar un proceso. Con frecuencia el output de un proceso forma directamente el Insumo del siguiente proceso.

La aplicación de un sistema de procesos dentro de una organización, junto con la identificación y las interacciones de estos procesos, y su gestión, puede considerarse un 'enfoque del proceso'.

Un enfoque del proceso para la gestión de la seguridad de la información presentado en este Estándar Internacional fomenta que sus usuarios enfaticen la importancia de:

a) entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información;
b) implementar y operar controles para manejar los riesgos de la seguridad de la información;
c) monitorear y revisar el desempeño y la efectividad del SGSI; y
d) mejoramiento continúo en base a la medición del objetivo.

Este Estándar Internacional adopta el modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA), el cual se puede aplicar a todos los procesos SGSI. La Figura 1 muestra cómo un SGSI

SOLO PARA FINES DIDACTICOS

toma como Insumo los requerimientos y expectativas de la seguridad de la información de las partes interesadas y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que satisfacen aquellos requerimientos y expectativas. La Figura 1 también muestra los vínculos en los procesos presentados en las Cláusulas 4, 5, 6, 7 y 8.

La adopción del modelo PDCA también reflejará los principios tal como se establecen en los Lineamientos OECD (2002)[1] que gobiernan los sistemas y redes de seguridad de la información. Este Estándar Internacional proporciona un modelo sólido para implementar los principios en aquellos lineamientos que gobiernan la evaluación del riesgo, diseño e implementación de seguridad, gestión y re-evaluación de la seguridad.

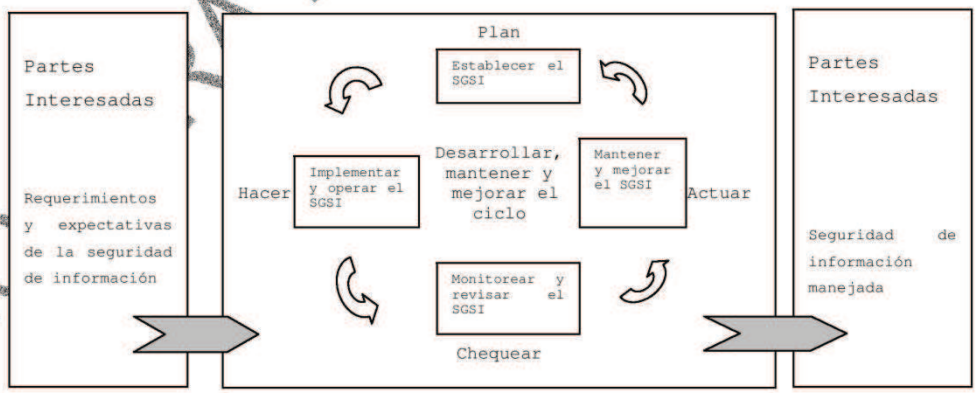
EJEMPLO 1

Un requerimiento podría ser que las violaciones de seguridad de la información no causen daño financiero a la organización y/o causen vergüenza a la organización.

EJEMPLO 2

Una expectativa podría ser que si ocurre un incidente serio –tal vez el pirateo del web site eBusiness de una organización- debería contarse con las personas con la capacitación suficiente en los procedimientos apropiados para minimizar el impacto.

Figura 1 – Modelo PDCA aplicado a los procesos SGSI



[1] Lineamientos OECD para Sistemas y Redes de Seguridad de la Información – Hacia una Cultura de Seguridad. Paris: OECD, Julio 2002. www.oecd.org.

SOLO PARA FINES DIDACTICOS

Planear (establecer el SGSI)	Establecer política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.
Hacer (implementar y operar el SGSI)	Implementar y operar la política, controles, procesos y procedimientos SGSI.
Chequear (monitorear y revisar el SGSI)	Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para su revisión.
Actuar (mantener y mejorar el SGSI)	Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoria interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.

0.3 Compatibilidad con otros sistemas de gestión

Este Estándar Internacional se alinea con el ISO 9001:2000 e ISO 14001:2004 para dar soporte a una implementación y operación consistente e integrada con los estándares de gestión relacionados. Por lo tanto, un sistema de gestión adecuadamente diseñado puede satisfacer los requerimientos de todos estos estándares. La Tabla C.1 muestra la relación entre las cláusulas de este Estándar Internacional, ISO 9001:2000 e ISO 14001:2004.

Este Estándar Internacional está diseñado para permitir que una organización se alinee o integre su SGSI con los requerimientos del sistema de gestión relacionado.

SOLO PARA FINES DIDACTICOS

Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos

Importante – No es el propósito de esta publicación incluir todas las provisiones necesarias de un contrato. Los usuarios son responsables de su correcta aplicación. El cumplimiento de un Estándar Internacional no quiere decir que confiere inmunidad de las obligaciones legales .

1 Alcance

1.1 General

Este Estándar Internacional abarca todos los tipos de organizaciones (por ejemplo; empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro). Este Estándar Internacional especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos comerciales generales de la organización. Especifica los requerimientos para la implementación de controles de seguridad personalizados para las necesidades de las organizaciones individuales o partes de ella.

El SGSI está diseñado para asegurar la selección adecuada y proporcionar controles de seguridad que protejan los activos de información y den confianza a las partes interesadas.

NOTA 1: Las referencias a 'comerciales' en este Estándar Internacional se deben implementar ampliamente para significar aquellas actividades que son básicas para los propósitos de la existencia de la organización.

NOTA 2: ISO/IEC 17799 proporciona un lineamiento de implementación que se puede utilizar cuando se diseñan controles.

1.2 Aplicación

Los requerimientos establecidos en este Estándar Internacional son genéricos y están diseñados para ser aplicables a todas las organizaciones, sin importar el tipo, tamaño y naturaleza. No es aceptable la exclusión de ninguno de los requerimientos especificados en las Cláusulas 4, 5, 6, y 8 cuando una organización asegura su conformidad con este Estándar Internacional.

SOLO PARA FINES DIDACTICOS

Cualquier exclusión de los controles vista como necesaria para satisfacer el criterio de aceptación del riesgo tiene que ser justificada y se debe proporcionar evidencia de que los riesgos asociados han sido aceptados por las personas responsables. Cuando se realizan exclusiones, las aseveraciones de conformidad con este estándar no son aceptables a no ser que estas exclusiones no afecten la capacidad y/o responsabilidad de la organización, para proporcionar seguridad de la información que satisfaga los requerimientos de seguridad determinados por la evaluación de riesgo y los requerimientos reguladores aplicables.

NOTA: Si una organización ya cuenta con un sistema de gestión de procesos comerciales operativos (por ejemplo, en relación con ISO 9001 o ISO 14001), en la mayoría de los casos es preferible satisfacer los requerimientos de este Estándar Internacional dentro de este sistema de gestión existente.

2 Referencias normativas

Los siguientes documentos mencionados son indispensables para la aplicación de este documento. Para referencias fechadas, sólo se aplica la edición citada. Para referencias no fechadas, se aplica la última edición del documento citado.

ISO/IEC 17799:2005, Tecnología de la información – Técnicas de seguridad – Código de práctica para la gestión de la seguridad de la información

3 Términos y definiciones

Para propósitos de este documento, se aplican los siguientes términos y definiciones.

3.1
activo

cualquier cosa que tenga valor para la organización
(ISO/IEC 13335-1:2004)

3.2
disponibilidad

la propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada
(ISO/IEC 13335-1:2004)

SOLO PARA FINES DIDACTICOS

3.3

confidencialidad

la propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no-autorizados

(ISO/IEC 13335-1:2004)

3.4

seguridad de información

preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad

(ISO/IEC 17799:2005)

3.5

evento de seguridad de la información

una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.

(ISO/IEC TR 18044:2004)

3.6

incidente de seguridad de la información

un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información.

(ISO/IEC TR 18044:2004)

3.7

sistema de gestión de seguridad de la información SGSI

esa parte del sistema gerencial general, basada en un enfoque de riesgo comercial; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información

NOTA: El sistema gerencial incluye la estructura organizacional, políticas, actividades de planeación, responsabilidades, prácticas, procedimientos, procesos y recursos

3.8

integridad

la propiedad de salvaguardar la exactitud e integridad de los activos.

(ISO/IEC 13335-1:2004)

SOLO PARA FINES DIDACTICOS

3.9

riesgo residual

el riesgo remanente después del tratamiento del riesgo
(ISO/IEC Guía 73:2002)

3.10

aceptación de riesgo

decisión de aceptar el riesgo
(ISO/IEC Guía 73:2002)

3.11

análisis de riesgo

uso sistemático de la información para identificar fuentes y para estimar el riesgo
(ISO/IEC Guía 73:2002)

3.12

valuación del riesgo

proceso general de análisis del riesgo y evaluación del riesgo
(ISO/IEC Guía 73:2002)

3.13

evaluación del riesgo

proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo
(ISO/IEC Guía 73:2002)

3.14

gestión del riesgo

actividades coordinadas para dirigir y controlar una organización con relación al riesgo
(ISO/IEC Guía 73:2002)

3.15

tratamiento del riesgo

proceso de tratamiento de la selección e implementación de medidas para modificar el riesgo
(ISO/IEC Guía 73:2002)
NOTA: En este Estándar Internacional el término 'control' se utiliza como sinónimo de 'medida'.

3.16

enunciado de aplicabilidad

SOLO PARA FINES DIDACTICOS

enunciado documentado que describe los objetivos de control y los controles que son relevantes y aplicables al SGSI de la organización.

NOTA: Los objetivos de control y controles se basan en los resultados y conclusiones de los procesos de tasación del riesgo y los procesos de tratamiento del riesgo, los requerimientos legales o reguladores, las obligaciones contractuales y los requerimientos comerciales de la organización para la seguridad de la información.

4 Sistema de gestión de seguridad de la información

4.1 Requerimientos generales

La organización debe establecer, implementar, operar, monitorear, mantener y mejorar continuamente un SGSI documentado dentro del contexto de las actividades comerciales generales de la organización y los riesgos que enfrentan. Para propósitos de este Estándar Internacional, los procesos utilizados se basan en el modelo PDCA que se muestra en la Figura 1.

4.2 Establecer y manejar el SGSI

4.2.1 Establecer el SGSI

La organización debe hacer lo siguiente:

a) Definir el alcance y los límites del SGSI en términos de las características del negocio, la organización, su ubicación, activos, tecnología e incluyendo los detalles de y la justificación de cualquier exclusión del alcance (ver 1.2).

b) Definir una política SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología que:

   1) incluya un marco referencial para establecer sus objetivos y establezca un sentido de dirección general y principios para la acción con relación a la seguridad de la información;

   2) tome en cuenta los requerimientos comerciales y legales o reguladores, y las obligaciones de la seguridad contractual;

   3) esté alineada con el contexto de la gestión riesgo estratégico de la organización en el cual se dará el establecimiento y mantenimiento del SGSI;

   4) establezca el criterio con el que se evaluará el riesgo (ver 4.2.1c);

   5) haya sido aprobada por la gerencia.

SOLO PARA FINES DIDACTICOS

NOTA: Para propósitos de este Estándar Internacional, la política SGSI es considerada como un super-conjunto de la política de seguridad de la información. Estas políticas se pueden describir en un documento.

c) Definir el enfoque de valuación del riesgo de la organización

1) Identificar una metodología de cálculo del riesgo adecuado para el SGSI y los requerimientos identificados de seguridad, legales y reguladores de la información comercial.

2) Desarrollar los criterios para aceptar los riesgos e identificar los niveles de riesgo aceptables (ver 5.1f).

La metodología de estimación del riesgo seleccionada debe asegurar que los cálculos del riesgo produzcan resultados comparables y reproducibles.

NOTA: Existen diferentes metodologías para el cálculo del riesgo. Los ejemplos de las metodologías de cálculo del riesgo se discuten en ISO/IEC TR 13335-3, Tecnología de información – Lineamiento para la gestión de la Seguridad TI – Técnicas para la gestión de la Seguridad TI

d) Identificar los riesgos

1) Identificar los activos dentro del alcance del SGSI y los propietarios[2] de estos activos.

2) Identificar las amenazas para aquellos activos.

3) Identificar las vulnerabilidades que podrían ser explotadas por las amenazas.

4) Identificar los impactos que pueden tener las pérdidas de confiabilidad, integridad y disponibilidad sobre los activos.

e) Analizar y evaluar el riesgo

1) Calcular el impacto comercial sobre la organización que podría resultar de una falla en la seguridad, tomando en cuenta las consecuencias de una pérdida de confidencialidad, integridad o disponibilidad de los activos.

2) Calcular la probabilidad realista de que ocurra dicha falla a la luz de las amenazas y vulnerabilidades prevalecientes, y los impactos asociados con estos activos, y los controles implementados actualmente.

3) Calcular los niveles de riesgo.

---

[2] El término 'propietario' identifica a la persona o entidad que tiene la responsabilidad gerencial aprobada de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término 'propietario' no significa que la persona tenga en realidad derechos de propiedad sobre el activo.

SOLO PARA FINES DIDACTICOS

4) Determinar si el riesgo es aceptable o requiere tratamiento utilizando el criterio de aceptación del riesgo establecido en 4.2.1 (c) (2).

f) Identificar y evaluar las opciones para el tratamiento de los riesgos

Las acciones posibles incluyen:

1) aplicar los controles apropiados;
2) aceptar los riesgos consciente y objetivamente, siempre que satisfagan claramente las políticas y el criterio de aceptación del riesgo (ver 4.2.1 c)2)) de la organización;
3) evitar los riesgos; y
4) transferir los riesgos comerciales asociados a otras entidades; por ejemplo: aseguradoras, proveedores.

g) Seleccionar objetivos de control y controles para el tratamiento de riesgos

Se deben seleccionar e implementar los objetivos de control y controles para cumplir con los requerimientos identificados por el proceso de tasación del riesgo y tratamiento del riesgo. Esta selección debe tomar en cuenta el criterio para aceptar los riesgos (ver 4.2.1(c), así como los requerimientos legales, reguladores y contractuales.

Se deben seleccionar los objetivos de control y los controles del Anexo A como parte de este proceso conforme sea apropiado para cubrir estos requerimientos.

Los objetivos de control y controles listados en el Anexo A no son exhaustivos y también se pueden seleccionar objetivos de control y controles adicionales.

NOTA: El Anexo A contiene una lista bastante completa de objetivos de control y controles comúnmente relevantes para las organizaciones. Se dirige a los usuarios de este Estándar Internacional como un punto de inicio para la selección de controles para asegurar que no se pase por alto ninguna opción de control importante.

h) Obtener la aprobación de la gerencia para los riesgos residuales propuestos.

i) Obtener la autorización de la gerencia para implementar y operar el SGSI.

j) Preparar un Enunciado de Aplicabilidad

Se debe preparar un Enunciado de Aplicabilidad que incluya lo siguiente:

1) los objetivos de control y los controles seleccionados en 4.2.1 (g) y las razones para su selección

2) los objetivos de control y controles implementados actualmente (ver 4.2.1 (e) 2); y

3) la exclusión de cualquier objetivo de control y control en el Anexo A y la justificación para su exclusión.

NOTA: El Enunciado de Aplicabilidad proporciona un resumen de las decisiones concernientes con el tratamiento del riesgo. El justificar las exclusiones proporciona un chequeo para asegurar que ningún control haya sido omitido inadvertidamente.

SOLO PARA FINES DIDACTICOS

4.2.2 Implementar y operar el SGSI

La organización debe hacer lo siguiente:

a) Formular un plan de tratamiento de riesgo que identifique la acción gerencial apropiada, los recursos, las responsabilidades y prioridades para manejar los riesgos de la seguridad de información (ver 5).

b) Implementar el plan de tratamiento de riesgo para poder lograr los objetivos de control identificados, los cuales incluyen tener en consideración el financiamiento y asignación de roles y responsabilidades.

c) Implementar los controles seleccionados en 4.2.1(g) para satisfacer los objetivos de control.

d) Definir cómo medir la efectividad de los controles o grupos de controles seleccionados y especificar cómo se van a utilizar estas mediciones para evaluar la efectividad del control para producir resultados comparables y reproducibles (ver 4.2.3 c)).
NOTA: La medición de la efectividad de los controles permite a los gerentes y personal determinar lo bien que los controles logran los objetivos de control planeados.

e) Implementar los programas de capacitación y conocimiento (ver 5.2.2).

f) Manejar las operaciones del SGSI.

g) Manejar recursos para el SGSI (ver 5.2).

h) Implementar los procedimientos y otros controles capaces de permitir una pronta detección de y respuesta a incidentes de seguridad.

4.2.3 Monitorear y revisar el SGSI

La organización debe hacer lo siguiente:

a) Ejecutar procedimientos de monitoreo y revisión, y otros controles para:
   1) detectar prontamente los errores en los resultados de procesamiento;
   2) identificar prontamente los incidentes y violaciones de seguridad fallidos y exitosos;
   3) permitir a la gerencia determinar si las actividades de seguridad delegadas a las personas o implementadas mediante la tecnología de información se están realizando como se esperaba;
   4) ayudar a detectar los eventos de seguridad, evitando así los incidentes de seguridad mediante el uso de indicadores; y
   5) determinar si son efectivas las acciones tomadas para resolver una violación de seguridad.

b) Realizar revisiones regulares de la efectividad del SGSI (incluyendo satisfacer la política y objetivos de seguridad del SGSI, y revisar los controles de seguridad) tomando en cuenta los resultados de auditorias de seguridad, incidentes, mediciones de seguridad, sugerencias y retroalimentación de todas las partes interesadas.

SOLO PARA FINES DIDACTICOS

c) Medir la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad.

d) Revisar las evaluaciones del riesgo a intervalos planeados y revisar el nivel de riesgo residual y riesgo aceptable identificado, tomando en cuenta los cambios en:
   1) la organización;
   2) tecnología;
   3) objetivos y procesos comerciales;
   4) amenazas identificadas;
   5) efectividad de los controles implementados; y
   6) eventos externos, como cambios en el ambiente legal o regulador, cambios en obligaciones contractuales y cambios en el clima social.

e) Realizar auditorias SGSI internas a intervalos planeados (ver 6).

NOTA: Las auditorías internas, algunas veces llamadas auditorías de primera persona, son realizadas por, o en representación de, la organización misma para propósitos internos.

f) Realizar una revisión gerencial del SGSI sobre una base regular para asegurar que el alcance permanezca adecuado y se identifiquen las mejoras en el proceso SGSI (ver 7.1).

g) Actualizar los planes de seguridad para tomar en cuenta los descubrimientos de las actividades de monitoreo y revisión.

h) Registrar las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño del SGSI (ver 4.3.3).

4.2.4 Mantener y mejorar el SGSI

La organización debe realizar regularmente lo siguiente:

a) Implementar las mejoras identificadas en el SGSI.

b) Tomar las acciones correctivas y preventivas apropiadas en concordancia con 8.2 y 8.3. Aplicar las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y aquellas de la organización misma.

c) Comunicar los resultados y acciones a todas las partes interesadas con un nivel de detalle apropiado de acuerdo a las circunstancias y, cuando sea relevante, acordar cómo proceder.

d) Asegurar que las mejoras logren sus objetivos señalados.

SOLO PARA FINES DIDACTICOS

4.3 Requerimientos de documentación

4.3.1 General

La documentación debe incluir los registros de las decisiones gerenciales, asegurar que las acciones puedan ser monitoreadas a las decisiones y políticas gerenciales, y los resultados registrados deben ser reproducibles.

Es importante ser capaces de demostrar la relación desde los controles seleccionados y de regreso a los resultados del proceso de evaluación del riesgo y tratamiento del riesgo, y subsecuentemente, de regreso a la política y objetivos del SGSI.

La documentación SGSI debe incluir lo siguiente:

a) enunciados documentados de la política SGSI (ver 4.2.1b)) y los objetivos;
b) el alcance del SGSI (ver 4.2.1a));
c) procedimientos y controles de soporte del SGSI;
d) una descripción de la metodología de evaluación del riesgo (ver 4.2.1c));
e) reporte de evaluación del riesgo (ver 4.2.1c) a 4.2.1g));
f) plan de tratamiento del riesgo (ver 4.2.2b));
g) Los procedimientos documentados necesarios por la organización para asegurar la planeación, operación y control de sus procesos de seguridad de la información y describir cómo medir la efectividad de los controles (ver 4.2.3c));
h) registros requeridos por este Estándar Internacional (ver 4.3.3); y
i) Enunciado de Aplicabilidad.

NOTA 1: Cuando aparece el término 'procedimiento documentado' dentro este Estándar Internacional, significa que el procedimiento se establece, documenta, implementa y mantiene.

NOTA 2: La extensión de la documentación SGSI puede diferir de una organización a otro debido a:

- el tamaño de la organización y el tipo de sus actividades; y
- el alcance y complejidad de los requerimientos de seguridad y el sistema que se está manejando.

NOTA 3: Los documentos y registros pueden estar en cualquier forma o medio.

4.3.2 Control de documentos

Los documentos requeridos por el SGSI deben ser protegidos y controlados. Se debe establecer un procedimiento documentado para definir las acciones gerenciales necesarias para:

a) aprobar la idoneidad de los documentos antes de su emisión;
b) revisar y actualizar los documentos conforme sea necesario y re-aprobar los documentos;
c) asegurar que se identifiquen los cambios y el status de la revisión actual de los documentos;

SOLO PARA FINES DIDACTICOS

d) asegurar que las versiones más recientes de los documentos relevantes estén disponibles en los puntos de uso;
e) asegurar que los documentos se mantengan legibles y fácilmente identificables;
f) asegurar que los documentos estén disponibles para aquellos que los necesitan; y sean transferidos, almacenados y finalmente eliminados en concordancia con los procedimientos aplicables para su clasificación;
g) asegurar que se identifiquen los documentos de origen externo;
h) asegurar que se controle la distribución de documentos;
i) evitar el uso indebido de documentos obsoletos; y
j) aplicarles una identificación adecuada si se van a retener por algún propósito.

4.3.3 Control de registros

Se deben establecer y mantener registros para proporcionar evidencia de conformidad con los requerimientos y la operación efectiva del SGSI. Deben ser protegidos y controlados. El SGSI debe tomar en cuenta cualquier requerimiento legal o regulador relevante. Los registros deben mantenerse legibles, fácilmente identificables y recuperables. Se deben documentar e implementar los controles necesarios para la identificación, almacenaje, protección, recuperación, tiempo de retención y disposición de los registros.

Se deben mantener registros del desempeño del proceso tal como se delinea en 4.2 y de todas las ocurrencias de incidentes de seguridad significativos relacionados con el SGSI.

EJEMPLO
Son ejemplos de registros los libros de visitantes, los registros de auditoria y las solicitudes de autorización de acceso.

5 Responsabilidad de la gerencia

5.1 Compromiso de la gerencia

La gerencia debe proporcionar evidencia de su compromiso con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoramiento del SGSI al:

a) establecer una política SGSI;
b) asegurar que se establezcan objetivos y planes SGSI;
c) establecer roles y responsabilidades para la seguridad de información;
d) comunicar a la organización la importancia de lograr los objetivos de seguridad de la información y cumplir la política de seguridad de la información, sus responsabilidades bajo la ley y la necesidad de un mejoramiento continuo;

SOLO PARA FINES DIDACTICOS

e) proporcionar los recursos suficientes para desarrollar, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI (ver 5.2.1);
f) decidir el criterio para la aceptación del riesgo y los niveles de riesgo aceptables;
g) asegurar que se realicen las auditorías internas SGSI (ver 6); y
h) realizar revisiones gerenciales del SGSI (ver 7).

5.2 Gestión de recursos

5.2.1 Provisión de recursos

La organización debe determinar y proporcionar los recursos necesarios para:

a) establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI;
b) asegurar que los procedimientos de seguridad de la información respalden los requerimientos comerciales;
c) identificar y tratar los requerimientos legales y reguladores y las obligaciones de seguridad contractuales;
d) mantener una seguridad adecuada mediante la correcta aplicación de todos los controles implementados;
e) llevar a cabo revisiones cuando sean necesarias, y reaccionar apropiadamente ante los resultados de estas revisiones;
f) donde se requiera, mejorar la efectividad del SGSI.

5.2.2 Capacitación, conocimiento y capacidad

La organización debe asegurar que todo el personal a quien se asignó las responsabilidades definidas en el SGSI sea competente para realizar las tareas requeridas para:

a) determinar las capacidades necesarias para el personal que realiza trabajo que afecta el SGSI;
b) proporcionar la capacitación o realizar otras acciones (por ejemplo; emplear el personal competente) para satisfacer estas necesidades;
c) evaluar la efectividad de las acciones tomadas;
d) mantener registros de educación, capacitación, capacidades, experiencia y calificaciones (ver 4.3.3).

La organización también debe asegurarse que todo el personal relevante esté consciente de la relevancia e importancia de sus actividades de seguridad de la información y cómo ellos pueden contribuir al logro de los objetivos SGSI.

SOLO PARA FINES DIDACTICOS

6 Auditorías internas SGSI

La organización debe realizar auditorías internas SGSI a intervalos planeados para determinar si los objetivos de control, controles, procesos y procedimientos del SGSI:

a) cumplen con los requerimientos de este Estándar Internacional y la legislación y regulaciones relevantes;
b) cumplen con los requerimientos de seguridad de la información identificados;
c) se implementan y mantienen de manera efectiva; y
d) se realizan conforme lo esperado.

Se debe planear un programa de auditoría tomando en consideración el status e importancia de los procesos y áreas a ser auditados, así como los resultados de auditorías previas. Se debe definir el criterio, alcance, frecuencia y métodos de auditoría. La selección de los auditores y la realización de las auditorías deben asegurar la objetividad e imparcialidad del proceso de auditoría. Los auditores no deben auditar su propio trabajo.

Las responsabilidades y requerimientos para la planeación y realización de las auditorías, y para el reporte de resultados y mantenimiento de registros (ver 4.3.3) se deben definir en un procedimiento documentado.

La gerencia responsable para el área siendo auditada debe asegurar que se den sin demora las acciones para eliminar las no-conformidades detectadas y sus causas. Las actividades de seguimiento deben incluir la verificación de las acciones tomadas y el reporte de los resultados de verificación (ver 8).

NOTA: ISO 19011:2002, Lineamiento para auditar sistemas de gestión de calidad y/o ambiental, puede proporcionar un lineamiento útil para llevar a cabo auditorías internas.

7 Revisión Gerencial del SGSI

7.1 General

La gerencia debe revisar el SGSI de la organización a intervalos planeados (por lo menos una vez al año) para asegurarse de su continua idoneidad, conveniencia y efectividad. Esta revisión debe incluir oportunidades de evaluación para el mejoramiento y la necesidad de cambios en el SGSI, incluyendo la política de seguridad y los objetivos de seguridad de la información. Los resultados de las revisiones deben documentarse claramente y se deben mantener registros (ver 4.3.3).

SOLO PARA FINES DIDACTICOS

7.2 Insumo de la revisión

El insumo para la revisión gerencial debe incluir:

a) resultados de auditorias y revisiones del SGSI;
b) retroalimentación de las partes interesadas;
c) técnicas, productos o procedimientos, que se podrían utilizar en la organización para mejorar el desempeño y efectividad del SGSI;
d) status de acciones preventivas y correctivas;
e) vulnerabilidades o amenazas no tratadas adecuadamente en la evaluación de riesgo previa;
f) resultados de mediciones de efectividad;
g) acciones de seguimiento de las revisiones gerenciales previas;
h) cualquier cambio que pudiera afectar el SGSI; y
i) recomendaciones para el mejoramiento.

7.3 Resultado de la revisión

El resultado de la revisión gerencial debe incluir cualquier decisión y acción relacionada con lo siguiente:

a) mejoramiento de la efectividad del SGSI;
b) actualización de la evaluación del riesgo y el plan de tratamiento del riesgo;
c) modificación de procedimientos y controles que afectan la seguridad de la información, si fuese necesario, para responder a eventos internos o externos que pudieran tener impacto sobre el SGSI, incluyendo cambios en:
    1) requerimientos comerciales;
    2) requerimientos de seguridad;
    3) procesos comerciales que afectan los requerimientos comerciales existentes;
    4) requerimientos reguladores o legales;
    5) obligaciones contractuales; y
    6) niveles de riesgo y/o criterio de aceptación del riesgo.
d) necesidades de recursos;
e) mejoramiento de cómo se mide la efectividad de los controles.

SOLO PARA FINES DIDACTICOS

8 Mejoramiento del SGSI

8.1 Mejoramiento continuo

La organización debe mejorar continuamente la efectividad del SGSI a través del uso de la política de seguridad de la información, objetivos de seguridad de la información, resultados de auditoria, análisis de los eventos monitoreados, acciones correctivas y preventivas, y la revisión gerencial.

8.2 Acción correctiva

La organización debe realizar las acciones para eliminar la causa de las no-conformidades con los requerimientos del SGSI para poder evitar la recurrencia. El procedimiento documentado para la acción correctiva debe definir los requerimientos para:

a) identificar las no-conformidades;
b) determinar las causas de las no-conformidades;
c) evaluar la necesidad de acciones para asegurar que las no-conformidades no vuelvan a ocurrir;
d) determinar e implementar la acción correctiva necesaria;
e) registrar los resultados de la acción tomada (ver 4.3.3); y
f) revisar la acción correctiva tomada.

8.3 Acción preventiva

La organización debe determinar la acción para eliminar la causa de las no-conformidades potenciales de los requerimientos SGSI para evitar su ocurrencia. Las acciones preventivas tomadas deben ser apropiadas para el impacto de los problemas potenciales. El procedimiento documentado para la acción preventiva debe definir los requerimientos para:

a) identificar las no-conformidades potenciales y sus causas;
b) evaluar la necesidad para la acción para evitar la ocurrencia de no-conformidades;
c) determinar e implementar la acción preventiva necesaria;
d) registrar los resultados de la acción tomada (ver 4.3.3); y
e) revisar la acción preventiva tomada.

La organización debe identificar los riesgos cambiados e identificar los requerimientos de acción preventiva enfocando la atención sobre los riesgos cambiados significativamente.

La prioridad de las acciones preventivas se debe determinar en base a los resultados de la evaluación del riesgo.

SOLO PARA FINES DIDACTICOS

NOTA La acción para evitar las no-conformidades con frecuencia es más una acción efectiva en costo que la acción correctiva.

SOLO PARA FINES DIDACTICOS

Anexo A

(Normativo)

Objetivos de control y controles

Los objetivos de control y los controles enumerados en la Tabla A.1 se derivan directamente de, y se alinean con, aquellos enumerados en BS ISO/IEC 17799:2005 Cláusulas del 5 al 15. Las listas en estas tablas no son exhaustivas y una organización podría considerar que son necesarios objetivos de control y controles adicionales. Los objetivos de control y los controles de estas tablas deben seleccionarse como parte del proceso SGSI especificado en 4.2.1.

El BS ISO/IEC 17799:2005 Cláusulas del 5 al 15 proporciona consulta y lineamientos para la implementación de las mejores prácticas en soporte de los controles especificados en A.5 al A.15.

Tabla A.1 – Objetivos de control y controles

A.5 Política de seguridad
A.5.1 Política de seguridad de información
Objetivo de control: Proporcionar dirección gerencial y apoyo a la seguridad

de la información en concordancia con los requerimientos comerciales y leyes y regulaciones relevantes		
A.5.1.1	Documentar política de seguridad de información	Control La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes.
A.5.1.2	Revisión de la política de seguridad de la información	Control La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.
A,6 Organización de la seguridad de la información		
A.6.1 Organización interna Objetivo: Manejar la seguridad de la información dentro de la organización.		
A.6.1.1	Compromiso de la gerencia con la seguridad de la información	Control La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información.
A.6.1.2	Coordinación de la seguridad de información	Control Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.
A.6.1.3	Asignación de responsabilidades de la seguridad de la información	Control Se deben definir claramente las responsabilidades de la seguridad de la información.
A.6.1.4	Proceso de autorización para los medios de procesamiento de información	Control Se debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento de información
A.6.1.5	Acuerdos de confidencialidad	Control Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la organización para la protección de la información.
A.6.1.6	Contacto con autoridades	Control Se debe mantener los contactos apropiados con las autoridades relevantes.
A.6.1.7	Contacto con grupos de interés especial	Control Se deben mantener contactos apropiados con los grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales.
A.6.1.8	Revisión independiente de la seguridad de la información	Control El enfoque de la organización para manejar la seguridad de la información y su implementación (es decir; objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se debe revisar independientemente a intervalos planeados, o cuando ocurran cambios significativos para la implementación de la seguridad.
A.6.2 Entidades externas		

SOLO PARA FINES DIDACTICOS

Objetivo: Mantener la seguridad de la información de la organización y los medios de procesamiento de información a los cuales entidades externas tienen acceso y procesan; o son comunicados a o manejados por entidades externas.		
A.6.2.1	Identificación de riesgos relacionados con entidades externas	Control Se deben identificar los riesgos que corren la información y los medios de procesamiento de información de la organización y se deben implementar los controles apropiados antes de otorgar acceso.
A.6.2.2	Tratamiento de la seguridad cuando se trabaja con clientes	Control Se deben tratar todos los requerimientos de seguridad identificados antes de otorgar a los clientes acceso a la información o activos de la organización.
A.6.2.3	Tratamiento de la seguridad en contratos con terceras personas	Control Los acuerdos que involucran acceso, procesamiento, comunicación o manejo por parte de terceras personas a la información o a los medios de procesamiento de información de la organización; agregar productos o servicios a los medios de procesamiento de la información deben abarcar los requerimientos de seguridad necesarios relevantes.
A.7 Gestión de activos		
A.7.1 *Responsabilidad por los activos* Objetivo: Lograr y mantener la protección apropiada de los activos organizacionales.		
A.7.1.1	Inventarios de activos	Control Todos los activos deben estar claramente identificados; y se debe elaborar y mantener un inventario de todos los activos importantes.
A.7.1.2	Propiedad de los activos	Control Toda la información y los activos asociados con los medios de procesamiento de la información deben ser 'propiedad'[3] de una parte designada de a organización.
A.7.1.3	Uso aceptable de los activos	Control Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.
A.7.2 Clasificación de la información Objetivo: Asegurar que a información reciba un nivel de protección apropiado.		
A.7.2.1	Lineamientos de clasificación	Control La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización.
A.7.2.2	Etiquetado y manejo de la información	Control Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización.

[3] Explicación: El término 'propietario' identifica a una persona o entidad que tiene la responsabilidad gerencial aprobada para controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término 'propietario' no significa que la persona tenga en realidad derechos de propiedad sobre el activo.

SOLO PARA FINES DIDACTICOS

A.8 Seguridad de los recursos humanos		
A.8.1 Antes del empleo[4] Objetivo: Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean adecuados para los roles para los cuales se les considera; y reducir el riesgo de robo, fraude o mal uso de los medios.		
A.8.1.1	Roles y responsabilidades	Control Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización.
A.8.1.2	Selección	Control Se deben llevar a cabo chequeos de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante, y deben ser proporcionales a los requerimientos comerciales, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.
A.8.1.3	Términos y condiciones de empleo	Control Como parte de su obligación contractual; los empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades y las de la organización para la seguridad de la información.
A.8.2 *Durante el empleo* Objetivo: Asegurar que todos los empleados, contratistas y terceros estén al tanto de las amenazas y inquietudes sobre la seguridad de información, sus responsabilidades y obligaciones, y que estén equipados para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir los riesgos de error humano.		
A.8.2.1	Gestión de responsabilidades	Control La gerencia debe requerir que los empleados, contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización.
A.8.2.2	Capacitación y educación en seguridad de la información	Control Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.
A.8.2.3	Proceso disciplinario	Control Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.
A.8.3 Terminación o cambio del empleo Objetivo: Asegurar que los empleados, contratistas y terceros salgan de una organización o cambien de empleo de una manera ordenada.		
A.8.3.1	Responsabilidades de terminación	Control Se deben definir y asignar claramente las

[4] Explicación: Aquí la palabra 'empleo' se utiliza para abarcar todas las siguientes situaciones diferentes: empleo de personas (temporal o larga duración), asignación de roles laborales, cambios de trabajo, asignación de contratos y la terminación de cualquiera de estos acuerdos.

SOLO PARA FINES DIDACTICOS

		responsabilidades para realizar la terminación o cambio del empleo.
A.8.3.2	Devolución de activos	Control Todos los empleados, contratistas y terceros deben devolver todos los activos de la organización que estén en su posesión a la terminación de su empleo, contrato o acuerdo.
A.8.3.3	Eliminación de derechos de acceso	Control Los derechos de acceso de todos los empleados, contratistas y terceros a la información y medios de procesamiento de la información deben ser eliminados a la terminación de su empleo, contrato o acuerdo, o se deben ajustar al cambio.
A.9 Seguridad física y ambiental		
A.7.1 *Áreas seguras* Objetivo: Evitar el acceso físico no autorizado, daño e interferencia al local y la información de la organización.		
A.9.1.1	Perímetro de seguridad física	Control Se debe utilizar perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger áreas que contienen información y medios de procesamiento de información.
A.9.1.2	Controles de entrada físicos	Control Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado.
A.9.1.3	Seguridad de oficinas, habitaciones y medios	Control Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones y medios.
A.9.1.4	Protección contra amenazas externas y ambientales	Control Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre.
A.9.1.5	Trabajo en áreas seguras	Control Se debe diseñar y aplicar protección física y lineamientos para trabajar en áreas seguras.
A.9.1.6	Áreas de acceso público, entrega y carga	Control Se deben controlar los puntos de acceso como las áreas de entrega y descarga y otros puntos donde personas no-autorizadas pueden ingresar a los locales, y cuando fuese posible, se deben aislar de los medios de procesamiento de la información para evitar un acceso no autorizado.
A.9.2 *Seguridad del equipo* Objetivo: Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización		
A.9.2.1	Ubicación y protección del equipo	Control El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.
A.9.2.2	Servicios públicos	Control El equipo debe ser protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.

SOLO PARA FINES DIDACTICOS

A.9.2.3	Seguridad en el cableado	Control El cableado de la energía y las telecomunicaciones que llevan data o sostienen los servicios de información deben ser protegidos de la intercepción o daño.
A.9.2.4	Mantenimiento de equipo	Control El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad.
A.9.2.5	Seguridad del equipo fuera-del-local	Control Se debe aplicar seguridad al equipo fuera-del-local tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización.
A.9.2.6	Eliminación seguro o re-uso del equipo	Control Todos los ítems de equipo que contengan medios de almacenaje deben ser chequeados para asegurar que se haya removido o sobre-escrito de manera segura cualquier data confidencial y software con licencia antes de su eliminación.
A.9.2.7	Traslado de Propiedad	Control Equipos, información o software no deben ser sacados fuera de la propiedad sin previa autorización.
A.10 Gestión de las comunicaciones y operaciones		
A.10.1 Procedimientos y responsabilidades operacionales Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información		
A.10.1.1	Procedimientos de operación documentados	Control Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten.
A.10.1.2	Gestión de cambio	Control Se deben controlar los cambios en los medios y sistemas de procesamiento de la información.
A.10.1.3	Segregación de deberes	Control Se deben segregar los deberes y áreas de responsabilidad para reducir las oportunidades de una modificación no-autorizada o no-intencionada o un mal uso de los activos de la organización.
A.10.1.4	Separación de los medios de desarrollo y operacionales	Control Se deben separar los medios de desarrollo, prueba y operacionales para reducir los riesgos de accesos no-autorizados o cambios en el sistema de operación.
A.10.2 Gestión de la entrega del servicio de terceros Objetivo: Implementar y mantener el nivel apropiado de seguridad de la información y entrega del servicio en línea con los contratos de entrega del servicio de terceros.		
A.10.2.1	Entrega del servicio	Control Se debe asegurar que los terceros implementen, operen y mantengan los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el contrato de entrega del servicio de terceros.
A.10.2.2	Monitoreo y revisión de los servicios de terceros	Control Los servicios, reportes y registros provistos por terceros deben ser monitoreados y revisados regularmente, y las auditorías se deben llevar a cabo regularmente.

SOLO PARA FINES DIDACTICOS

A.10.2.3	Manejar los cambios en los servicios de terceros	Control Se deben manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejoramiento de las políticas, procedimientos y controles de seguridad existentes, tomando en cuenta el grado crítico de los sistemas y procesos comerciales involucrados y la re-evaluación de los riesgos.
A.10.3 Planeación y aceptación del sistema Objetivo: Minimizar el riesgo de fallas en los sistemas.		
A.10.3.1	Gestión de capacidad	Control Se deben monitorear, afinar y realizar proyecciones del uso de los recursos para asegurar el desempeño del sistema requerido.
A.10.3.2	Aceptación del sistema	Control Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cabo pruebas adecuadas del(los) sistema(s) durante su desarrollo y antes de su aceptación.
A.10.4 *Protección contra software malicioso y código móvil* Objetivo: Proteger la integridad del software y la información.		
A.10.4.1	Controles contra software malicioso	Control Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos malicioso y se deben implementar procedimientos de conciencia apropiados.
A.10.4.2	Controles contra códigos móviles	Control Cuando se autoriza el uso de un código móvil, a configuración debe asegurar que el código móvil autorizado opere de acuerdo a una política de seguridad claramente definida, y se debe evitar que se ejecute un código móvil no-autorizado
A.10.5 Respaldo (back-up) Objetivo: Mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones.		
A.10.5.1	*Back-up o respaldo de la información*	Control Se deben realizar copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente de acuerdo a la política.
A.10.6 *Gestión de seguridad de redes* Objetivo: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.		
A.10.6.1	Controles de red	Control Las redes deben ser adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.
A.10.6.2	Seguridad de los servicios de red	Control Se deben identificar los dispositivos de seguridad, niveles de servicio y los requerimientos e incluirlos en cualquier contrato de servicio de red, ya sea que estos servicios sean provistos en-casa o sean abastecidos externamente.
A.10.7 Gestión de medios		

SOLO PARA FINES DIDACTICOS

Objetivo: Evitar la divulgación, modificación, eliminación o destrucción no-autorizada de los activos; y la interrupción de las actividades comerciales.		
A.10.7.1	Gestión de los medios removibles	Control Deben existir procedimientos para la gestión de medios removibles.
A.10.7.2	Eliminación de medios	Control Los medios deben ser eliminados utilizando procedimientos formales y de una manera segura cuando ya no se les requiere.
A.10.7.3	Procedimientos de manejo de la información	Control Se deben establecer los procedimientos para el manejo y almacenaje de la información para proteger dicha información de una divulgación no autorizada o un mal uso.
A.10.7.4	Seguridad de documentación del sistema	Control Se debe proteger la documentación de un acceso no autorizado.
A.10.8 Intercambio de información Objetivo: Mantener la seguridad de la información y software intercambiados dentro de una organización y con cualquier entidad externa.		
A.10.8.1	Procedimientos y políticas de información y software	Control Se deben establecer política, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación.
A.10.8.2	Acuerdos de intercambio	Control Se deben establecer acuerdos para el intercambio de información y software entre la organización y entidades externas.
A.10.8.3	Medios físicos en tránsito	Control Los medios que contienen información deben ser protegidos contra un acceso no-autorizado, mal uso o corrupción durante el transporte más allá de los límites físicos de una organización.
A.10.8.4	Mensajes electrónicos	Control Se debe proteger adecuadamente los mensajes electrónicos.
A.10.8.5	Sistemas de información comercial	Control Se deben desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información comercial.
A.10.9 Servicios de comercio electrónico Objetivo: Asegurar la seguridad de los servicios de comercio electrónico y su uso seguro		
A.10.9.1	Comercio electrónico	Control Se debe proteger la información involucrada en el comercio electrónico que se trasmite a través de redes públicas de cualquier actividad fraudulenta, disputa contractual y divulgación y modificación no autorizada.
A.10.9.2	Transacciones en-línea	Control Se debe proteger la información involucrada en las transacciones en-línea para evitar la transmisión incompleta, rutas equivocadas, alteración no-autorizada del mensaje, divulgación no-autorizada, y duplicación o re-envío no-autorizado del mensaje.
A.10.9.3	Información	Control

SOLO PARA FINES DIDACTICOS

	disponible públicamente	Se debe proteger la integridad de la información disponible públicamente para evitar la modificación no autorizada.
A.10.10 Monitoreo Objetivo: Detectar actividades de procesamiento de información no autorizadas.		
A.10.10.1	*Registro de auditoria*	Control Se deben producir registros de la actividades de auditoria, excepciones y eventos de seguridad de la información y se deben mantener durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso.
A.10.10.2	*Uso del sistema de monitoreo*	Control Se deben establecer procedimientos para monitorear el uso de los medios de procesamiento de información y el resultado de las actividades de monitoreo se debe revisar regularmente.
A.10.10.3	Protección de la información del registro	Control Se deben proteger los medios de registro y la información del registro contra alteraciones y acceso no-autorizado.
A.10.10.4	Registros del administrador y operador	Control Se deben registrar las actividades del administrador y operador del sistema.
A.10.10.5	Registro de fallas	Control Las fallas se deben registrar, analizar y se debe tomar la acción apropiada.
A.10.10.6	Sincronización de relojes	Control Los relojes de los sistemas de procesamiento de información relevantes de una organización o dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta acordada.
A.11 Control de acceso		
A.11.1 Requerimiento comercial para el control del acceso Objetivo: Controlar acceso a la información		
A.11.1.1	Política de control de acceso	Control Se debe establecer, documentar y revisar la política de control de acceso en base a los requerimientos de seguridad y comerciales.
A.11.2 Gestión del acceso del usuario Objetivo: Asegurar el acceso del usuario autorizado y evitar el acceso no-autorizado a los sistemas de información.		
A.11.2.1	Inscripción del usuario	Control Debe existir un procedimiento formal para la inscripción y des-inscripción para otorgar acceso a todos los sistemas y servicios de información.
A.11.2.2	Gestión de privilegios	Control Se debe restringir y controlar la asignación y uso de los privilegios.
A.11.2.3	Gestión de la clave del usuario	Control La asignación de claves se debe controlar a través de un proceso de gestión formal.
A.11.2.4	Revisión de los derechos de acceso del usuario	Control La gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.
A.11.3 Responsabilidades del usuario Objetivo: Evitar el acceso de usuarios no autorizados, y el compromiso o robo de la información y los medios de procesamiento de la información.		

SOLO PARA FINES DIDACTICOS

A.11.3.1	Uso de clave	Control Se debe requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves.
A.11.3.2	Equipo de usuario desatendido	Control Se debe requerir que los usuarios se aseguren de dar la protección apropiada al equipo desatendido
A.11.3.3	Política de pantalla y escritorio limpio	Control Se debe adoptar una política de escritorio limpio para los documentos y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.
A.11.4 Control de acceso a redes Objetivo: Evitar el acceso no-autorizado a los servicios en red.		
A.11.4.1	Política sobre el uso de servicios en red	Control Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.
A.11.4.2	Autenticación del usuario para conexiones externas	Control Se debe utilizar métodos de autenticación para controlar el acceso de usuarios remotos.
A.11.4.3	Identificación del equipo en red	Control Se debe considerar la identificación automática del equipo como un medio para autenticar las conexiones desde equipos y ubicaciones específicas.
A.11.4.4	Protección del puerto de diagnóstico remoto	Control Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y configuración.
A.11.4.5	Segregación en redes	Control Los servicios de información, usuarios y sistemas de información se deben segregar en las redes.
A.11.4.6	Control de conexión de redes	Control Se debe restringir la capacidad de conexión de los usuarios en las redes compartidas, especialmente aquellas que se extienden a través de los límites organizaciones, en concordancia con la política de control de acceso y los requerimientos de las aflicciones comerciales (ver 11.1).
A.11.4.7	Control de 'routing' de redes	Control Se deben implementar controles 'routing' para las redes para asegurar que las conexiones de cómputo y los flujos de información no infrinjan la política de control de acceso de las aplicaciones comerciales.
A.11.5 Control de acceso al sistema de operación Objetivo: Evitar acceso no autorizado a los sistemas operativos.		
A.11.5.1	Procedimientos de registro en el terminal	Control Se debe controlar el acceso los servicios operativos mediante un procedimiento de registro seguro.
A.11.5.2	Identificación y autenticación del usuario	Control Todos los usuarios deben tener un identificador singular (ID de usuario) para su uso personal y exclusivo, se debe elegir una técnica de autenticación adecuada para verificar la

SOLO PARA FINES DIDACTICOS

		identidad del usuario.
A.11.5.3	Sistema de gestión de claves	Control Los sistemas de manejo de claves deben ser interactivos y deben asegurar la calidad de las claves.
A.11.5.4	Uso de utilidades del sistema	Control Se debe restringir y controlar estrictamente el uso de los programas de utilidad que podrían superar al sistema y los controles de aplicación.
A.11.5.5	Sesión inactiva	Control Las sesiones inactivas deben cerrarse después de un período de inactividad definido.
A.11.5.6	Limitación de tiempo de conexión	Control Se debe utilizar restricciones sobre los tiempos de conexión para proporcionar seguridad adicional a las aplicaciones de alto riesgo.
A.11.6 Control de acceso a la aplicación e información Objetivo: Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.		
A.11.6.1	Restricción al acceso a la información	Control Se debe restringir el acceso de los usuarios y personal de soporte al sistema de información y aplicación en concordancia con la política de control de acceso definida.
A.11.6.2	Aislamiento del sistema sensible	Control Los sistemas sensibles deben tener un ambiente de cómputo dedicado (aislado).
A.11.7 Computación móvil y tele-trabajo Objetivo: Asegurar la seguridad de la información cuando se utilice medios computación móvil y tele-trabajo.		
A.11.7.1	Computación móvil y comunicaciones	Control Se debe establecer una política formal y adoptar las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móviles.
A.11.7.2	Tele-trabajo	Control Se deben desarrollar e implementar políticas, planes operacionales y procedimientos para actividades de tele-trabajo.
A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información		
A.12.1 Requerimientos de seguridad de los sistemas Objetivo: Asegurar que la seguridad sea una parte integral de los sistemas de información.		
A.12.1.1	Análisis y especificación de los requerimientos de seguridad	Control Los enunciados de los requerimientos comerciales para sistemas nuevos, o mejorar los sistemas existentes deben especificar los requerimientos de los controles de seguridad.
A.12.2 Procesamiento correcto en las aplicaciones Objetivo: Evitar errores, pérdida, modificación no-autorizada o mal uso de la información en las aplicaciones.		
A.12.2.1	Validación de data de Insumo	Control El Insumo de data en las aplicaciones debe ser validado para asegurar que esta data sea correcta y apropiada.
A.12.2.2	Control de procesamiento interno	Control Se deben incorporar chequeos de validación en las aplicaciones para detectar cualquier corrupción de la información a través de errores de

SOLO PARA FINES DIDACTICOS

		procesamiento o actos deliberados.
A.12.2.3	Integridad del mensaje	Control Se deben identificar los requerimientos para asegurar la autenticidad y protección de la integridad de mensaje en las aplicaciones, y se deben identificar e implementar los controles apropiados.
A.12.2.4	Validación de data de output	Control Se debe validar el output de data de una aplicación para asegurar que el procesamiento de la información almacenada sea correcto y apropiado para las circunstancias.
A.12.3 Controles criptográficos Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información a través de medios criptográficos.		
A.12.3.1	Política sobre el uso de controles criptográficos	Control Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.12.3.2	Gestión clave	Control Se debe utilizar una gestión clave para dar soporte al uso de las técnicas de criptografía en la organización.
A.12.4 Seguridad de los archivos del sistema Objetivo: Garantizar la seguridad de los archivos del sistema		
A.12.4.1	Control de software operacional	Control Se debe contar con procedimientos para controlar la instalación de software en los sistemas operacionales.
A.12.4.2	Protección de la data de prueba del sistema	Control Se debe seleccionar cuidadosamente, proteger y controlar la data de prueba
A.12.4.3	Control de acceso al código fuente del programa	Control Se debe restringir el acceso al código fuente del programa.
A.12.5 Seguridad en los procesos de desarrollo y soporte Objetivo: Mantener la seguridad del software e información del sistema de aplicación		
A.12.5.1	Procedimientos de control de cambio	Control La implementación de cambios se debe controlar mediante el uso de procedimientos formales de control de cambios.
A.12.5.2	Revisión técnica de las aplicaciones después de cambios en el sistema operativo	Control Cuando se cambian los sistemas operativos, se deben revisar y probar las aplicaciones críticas del negocio para asegurar que no exista un impacto adverso en las operaciones o seguridad organizacional.
A.12.5.3	Restricciones sobre los cambios en los paquetes de software	Control No se deben fomentar las modificaciones a los paquetes de software, se deben limitar a los cambios necesarios y todos los cambios deben ser controlados estrictamente.
A.12.5.4	Filtración de información	Control Se deben evitar las oportunidades de filtraciones en la información.
A.12.5.5	Desarrollo de outsourced software	Control El desarrollo de software que ha sido outsourced debe ser supervisado y monitoreado por la

SOLO PARA FINES DIDACTICOS

		organización.
A.12.6 Gestión de vulnerabilidad técnica Objetivo: Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas.		
A.12.6.1	Control de vulnerabilidades técnicas	Control Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso; se debe evaluar la exposición de la organización ante esas vulnerabilidades; y se deben tomar las medidas apropiadas para tratar el riesgo asociado.
A. 13 Gestión de incidentes en la seguridad de la información		
A.13.1 Reporte de eventos y debilidades en la seguridad de la información Objetivo: Asegurar que la información de los eventos y debilidades en la seguridad de la información asociados con los sistemas de información sea comunicada de una manera que permita tomar una acción correctiva oportuna.		
A.13.1.1	Reporte de eventos en la seguridad de la información	Control Los eventos de seguridad de la información deben reportarse a través de los canales gerenciales apropiados lo más rápidamente posible.
A.13.1.2	Reporte de debilidades en la seguridad	Control Se debe requerir que todos los empleados, contratistas y terceros usuarios de los sistemas y servicios de información tomen nota y reporten cualquier debilidad observada o sospechada en la seguridad de los sistemas o servicios.
A.13.2 Gestión de incidentes y mejoras en la seguridad de la información Objetivo: Asegurar que se aplique un enfoque consistente y efectivo a la gestión de la seguridad de la información.		
A.13.2.1	Responsabilidades y procedimientos	Control Se deben establecer las responsabilidades y procedimientos gerenciales para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.
A.13.2.2	Aprendizaje de los incidentes en la seguridad de la información	Control Deben existir mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información.
A.13.2.3	Recolección de evidencia	Control Cuando la acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (sea civil o criminal), se debe recolectar, mantener y presentar evidencia para cumplir las reglas de evidencia establecidas en la(s) jurisdicción(es) relevantes.
A.14 Gestión de la continuidad comercial		
A.14.1 Aspectos de la seguridad de la información de la gestión de la continuidad comercial Objetivo: Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas o desastres importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.		
A.14.1.1	Incluir seguridad de la información en el proceso de gestión de	Control Se debe desarrollar y mantener un proceso gerencial para la continuidad del negocio a través de toda la organización para tratar los

SOLO PARA FINES DIDÁCTICOS

	continuidad comercial	requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización.
A.14.1.2	Continuidad comercial y evaluación del riesgo	Control Se deben identificar los eventos que causan interrupciones en los procesos comerciales, junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.
A.14.1.3	Desarrollar e implementar planes de continuidad incluyendo seguridad de la información	Control Se deben desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla en los procesos comerciales críticos.
A.14.1.4	Marco referencial para la planeación de la continuidad comercial	Control Se debe mantener un solo marco referencial de planes de continuidad comercial para asegurar que todos los planes sean consistentes y para tratar consistentemente los requerimientos de la seguridad de la información e identificar las prioridades de pruebas y mantenimiento.
A.14.1.5	Prueba, mantenimiento y re-evaluación de planes de continuidad comerciales	Control Los planes de continuidad comercial se deben probar y actualizar regularmente para asegurar que estén actualizados y sean efectivos.
A.15 Cumplimiento		
A.15.1 Cumplimiento con requerimientos legales Objetivo: Evitar violaciones de cualquier ley, obligación reguladora o contractual y de cualquier requerimiento de seguridad		
A.15.1.1	Identificación de legislación aplicable	Control Se deben definir explícitamente, documentar y actualizar todos los requerimientos estatutarios, reguladores y contractuales y el enfoque de la organización relevante para cada sistema de información y la organización.
A.15.1.2	Derechos de propiedad intelectual (IPR)	Control Se deben implementar los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso de material con respecto a los derechos de propiedad intelectual y sobre el uso de los productos de software patentados.
A.15.1.3	Protección los registros organizacionales	Control Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales.
A.15.1.4	Protección de data y privacidad de información personal	Control Se deben asegurar la protección y privacidad tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.

SOLO PARA FINES DIDACTICOS

A.15.1.5	Prevención de mal uso de medios de procesamiento de información	Control Se debe desanimar a los usuarios de utilizar los medios de procesamiento de la información para propósitos no-autorizados.
A.15.1.6	Regulación de controles criptográficos	Control Se deben utilizar controles en cumplimiento con los acuerdos, leyes y regulaciones relevantes.
A.15.2 Cumplimiento con las políticas y estándares de seguridad, y el cumplimiento técnico Objetivo: Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.		
A.15.2.1	*Cumplimiento con las políticas y estándares de seguridad*	Control Los gerentes deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad sean realizados correctamente en cumplimiento con las políticas y estándares de seguridad.
A.15.2.2	*Chequeo de cumplimiento técnico*	Control Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.
A.15.3 Consideraciones de auditoria de los sistema de información Objetivo: Maximizar la efectividad de y minimizar la interferencia de/desde el proceso de auditoria de los sistema de información.		
A.15.3.1	Controles de auditoria de sistemas de información	Control Se deben planear cuidadosamente los requerimientos y actividades de las auditorias que involucran chequeo de los sistemas operacionales y se debe acordar minimizar el riesgo de interrupciones en los procesos comerciales.
A.15.3.2	Protección de las herramientas de auditoria de los sistemas de información	Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar cualquier mal uso o compromiso posible.

SOLO PARA FINES DIDACTICOS

Anexo B

(Informativo)

Principios OECD y este Estándar Internacional

Los principios dados en los Lineamientos OECD para la Seguridad de los Sistemas y Redes de Información [1] se aplican a toda las políticas y niveles operacionales que gobiernan la seguridad de los sistemas y redes de información. Este Estándar Británico proporciona un marco referencial del sistema de gestión de la seguridad de la información para implementar algunos de los principios OECD utilizando el modelo PDCA y los procesos descritos en las Cláusulas 4, 5, 6 y 8 como se indica en la Tabla B.1.

Tabla B.1 – Principios OECD y el modelo PDCA

Principio OECD	Proceso SGSI correspondiente y fase PDCA
Conciencia	Esta actividad es parta de la fase **Hacer**

Los participantes deben estar al tanto de la necesidad de seguridad de los sistemas y redes de información y lo que pueden hacer para aumentar la seguridad	(ver 4.2.2 y 5.2.2)
Responsabilidad Todos los participantes son responsables de la seguridad de los sistemas y redes de información.	Esta actividad es parte de la fase **Hacer** (ver 4.2.2 y 5.1)
Respuesta Los participantes deben actuar de manera oportuna y cooperativa para evitar, detectar y responder a los incidentes de seguridad.	Esta es en parte una actividad de monitoreo de la fase **Chequear** (ver 4.2.3 y 6 al 7.3) y una actividad de respuesta de la fase **Actuar** (ver 4.2.4 y 8.1 al 8.3). Esto también puede ser abarcado por algunos aspectos de las fases **Planear** y **Chequear.**
Evaluación del riesgo Los participantes deben realizar evaluaciones de riesgo.	Esta actividad es una parte de la fase **Planear** (ver 4.2.1) y la evaluación del riesgo es parte de la fase **Chequear** (ver 4.2.3 y 6 al 7.3).
Diseño e implementación de la seguridad Los participantes deben incorporar la seguridad como un elementos esencial de los sistemas y redes de información.	Una vez que se ha completado la evaluación del riesgo, se seleccionan los controles para el tratamiento de riesgos como una parte de la fase **Planear** (ver 4.2.1). La fase **Hacer** (ver 4.2.2 y 5.2) entonces abarca la implementación y uso operacional de estos controles.
Gestión de la seguridad Los participantes deben adoptar un enfoque integral para la gestión de la seguridad.	La gestión del riesgo es un proceso que incluye la prevención, detección y respuesta a los incidentes, mantenimiento continuo, revisión y auditoria. Todos estos aspectos son parte de las fases **Planear, Hacer, Chequear y Actuar.**
Reevaluación Los participantes deben revisar y reevaluar la seguridad de los sistemas y redes de información, y realizar las modificaciones apropiadas a las políticas, prácticas, medidas y procedimientos.	La reevaluación de la seguridad de la información es una parte de la fase **Chequear** (ver 4.2.3 y 6 a 7.3) donde se deben realizar revisiones regulares para chequear la efectividad del sistema de gestión de seguridad de la información, y mejorar la seguridad es parte de la fase **Actuar** (ver 4.2.4 y 8.1 al 8.3).

SOLO PARA FINES DIDACTICOS

Anexo C

(Informativo)

Correspondencia entre ISO 9001:2000, ISO 14001:2004 y este Estándar Internacional

La tabla C.1 muestra la correspondencia entre ISO 9001:2000, ISO 14001:2004 y este Estándar Internacional

Tabla C.1 – Correspondencia entre ISO 9001:2000, ISO 14001:2004 y este Estándar Internacional

Este Estándar Internacional	ISO 9001:2000	ISO 14001:2004
Introducción General Enfoque del proceso Compatibilidad con otros sistemas de gestión	**0 Introducción** 0.1 General 0.2 Enfoque del proceso 0.3 Relación con ISO 9004 0.4 Compatibilidad con otros sistemas de gestión	**Introducción**
1 Alcance 1.1 General 1.2 Aplicación	**1 Alcance** 1.1 General 1.2 Aplicación	**1 Alcance**
2 Referencias normativas	**2 Referencia normativa**	**2 Referencia normativa**
3 Términos y definiciones	**3 Términos y definiciones**	**3 Términos y definiciones**
4 Sistema de gestión de la seguridad de la información 4.1 Requerimientos generales 4.2 Establecer y manejar el SGSI 4.2.1 Establecer el SGSI 4.2.2 Implementar y operar el SGSI 4.2.3 Monitorear y revisar el SGSI 4.2.4 Mantener y mejorar el SGSI 4.3 Requerimientos de documentación 4.3.1 General 4.3.2 Control de documentos 4.3.3 Control de registros	**4 Sistema de gestión de calidad** 4.1 Requerimientos generales 8.2.3 Monitoreo y medición de procesos 8.2.4 Monitoreo y medición del producto 4.2 Requerimientos de documentación 4.2.1 General 4.2.2 Manual de calidad 4.2.3 Control de documentos 4.2.4 Control de registros	**4 Requerimientos EMS** 4.1 Requerimientos generales 4.4 Implementación y operación 4.5.1 Monitoreo y medición 4.4.5 Control de documentación 4.5.4 Control de registros
5 Responsabilidad de gestión 5.1 Compromiso de la gerencia	**5 Responsabilidad de gestión** 5.1 Compromiso de la gerencia 5.2 Enfoque del cliente 5.3 Política de calidad 5.4 Planeación 5.5 Responsabilidad, autoridad y comunicación	 4.2 Política ambiental 4.3 Planeación
5.2 Manejo de recursos 5.2.1 Provisión de recursos 5.2.2 Capacitación, conciencia y capacidad	**6 Manejo de recursos** 6.1 Provisión de recursos 6.2 Recursos humanos 6.2.2 Capacidad, conciencia y capacitación 6.3 Infraestructura 6.4 Ambiente laboral	 4.4.2 Competencia, capacitación y conciencia
6 Auditorías internas SGSI	8.2.2 Auditoría interna	4.5.5 Auditoría interna

39

SOLO PARA FINES DIDACTICOS

7 Revisión gerencial del SGSI 7.1 General 7.2 Insumo de la revisión 7.3 Output de la revisión	**5.6 Revisión gerencial** 5.6.1 General 5.6.2 Insumo de la revisión 5.6.3 Output de la revisión	**4.6 Revisión gerencial**
8 Mejoramiento SGSI 8.1 Mejoramiento continuo 8.2 Acción correctiva 8.3 Acción preventiva	**8.5 Mejoramiento** 8.5.2 Mejoramiento continuo 8.5.3 Acciones correctivas 8.5.3 Acciones preventivas	 4.5.3 No-conformidad y acción correctiva y preventiva
Anexo A Objetivos de control y controles **Anexo B Principios OECD y este Estándar Internacional** **Anexo C Correspondencia entre ISO 9001:2000, ISO 14001:2004 y este Estándar Internacional**	 **Anexo A Correspondencia entre ISO 9001:2000 e ISO 14001:1996**	**Anexo A Lineamiento sobre el uso de este Estándar Internacional** **Anexo B Correspondencia entre ISO 14001:2004 e ISO 9001_2000**

Bibliografía

Publicación de estándares

(1) ISO 9001:2000, Sistemas de gestión de calidad - Requerimientos

(2) ISO/IEC 13335-1:204, Tecnología de la información – Técnicas de seguridad – Gestión de seguridad en tecnología de información y comunicaciones – Parte 1: Conceptos y modelos para la gestión de seguridad en la tecnología de la información y comunicaciones

(3) ISO/IEC TR 13335-3:1998, *Lineamientos para la Gestión de Seguridad TI – Parte 3: Técnicas para la gestión de la seguridad TI*

(4) ISO/IEC 13335-4:2000, *Lineamientos para la Gestión de la Seguridad TI – Parte 4: Selección de salvaguardas*

(5) ISO 14001:2004, Sistemas de gestión ambiental – Requerimientos con lineamiento para su uso

(6) ISO/IEC TR 18044:2004, Tecnología de la información – Técnicas de seguridad – Gestión de incidentes en la seguridad de la información

(7) ISO/IEC 19011:2002, Lineamientos para la auditoría de sistemas de auditoría y/o gestión ambiental

(8) ISO/IEC Guía 62:1996, *Requerimientos generales para los organismos que operan la evaluación y certificación/registro de sistemas de calidad.*

(9) ISO/IEC Guía 73:2002, Gestión de riesgo –Vocabulario – Lineamientos para el uso en estándares

Otras publicaciones

(1) OECD, *Lineamientos OECD para la Seguridad de los Sistemas y Redes de Información – Hacia una Cultura de Seguridad.* Paris: OECD, Julio 2002, www.oecd.org

(2) NIST SP 800-30, Guía de Gestión de Riesgo para los Sistemas de Tecnología de la Información

(3) Deming, W.E., Fuera de la Crisis, Cambridge, Mass:MIT, Centro de Estudios de Ingeniería Avanzada, 1986

SOLO PARA FINES DIDACTICOS