TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo

Hans Ryan Espinoza Aguinaga

20047270

ASESOR: Dr. Manuel Tupia Anticona.

Lima, Octubre 2013

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

RESÚMEN

En los últimos 20 años la información se ha convertido en un activo muy importante y crucial dentro de las organizaciones. Por esta razón la organización tiene la necesidad de protegerla si es que la información tiene relación ya sea con el negocio o con sus clientes.

Para gestionar la información y su seguridad, las entidades pueden adoptar alguna de las normas y buenas prácticas existentes en el mercado.

Para el caso de una empresa del rubro de producción y distribución de alimentos de consumo masivo, también aplica esta necesidad de proteger la información. Por ejemplo, en unos de sus principales procesos que es el de *producción*, está implicada información de gran importancia para la empresa, como "recetas" de productos, programación de manufactura, sistemas que se usan, tipos de pruebas de calidad de producto, etc., la cual debe estar resguardada correctamente para evitar que dicha información se pierda o caiga en manos indebidas y así garantizar que se logren los objetivos del negocio.

En el presente proyecto de fin de carrera se tomaran en cuenta los aspectos más importantes de la norma ISO/IEC 27001:2005, a partir de los cuales se buscará poder desarrollar cada una de las etapas del diseño de un sistema de gestión de seguridad de información para que pueda ser empleado por una *empresa dedicada a la producción de alimentos de consumo masivo* en el Perú, lo cual permitirá que ésta cumpla con las normas de regulación vigentes en lo que respecta a seguridad de información.

Para efectos del análisis de riesgos para este proyecto de tesis, se decidió trabajar con el proceso de producción, ya que se consideró que era el proceso más importante dentro del funcionamiento de la empresa. Este proceso de producción a su vez se dividió en 4 subprocesos que lo conforman, los cuales fueron el proceso de *planificación, manufactura, calidad y bodegas e inventarios.*

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

INDICE

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

INDICE DE TABLAS

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

INDICE DE ILUSTRACIONES

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

CAPÍTULO 1 PREMISAS Y PLANIFICACIÓN DEL PROYECTO

En este capítulo se desarrollo la introducción de este proyecto de fin de carrera, definiendo primero la problemática que se desea solucionar con este proyecto, objetivos, resultados esperados, alcance, los métodos a utilizar durante este trabajo, la justificación y viabilidad de realizar este trabajo, el marco conceptual y teórico y por último el estado del arte de la solución planteada.

1.1 INTRODUCCIÓN

En los últimos 20 años, con el desarrollo de la tecnología, la información se ha convertido en uno de los activos más importantes dentro de las empresas, pudiendo estar presente en múltiples formatos: papel, almacenada electrónicamente, ilustrada en películas, hablada en conversaciones o transmitida por alguna tecnología de comunicaciones, entre otros. [1]

Debido a esto, las empresas en la actualidad han reducido cada vez más sus inversiones en la compra de productos y herramientas tecnológicas, destinando más bien parte de su presupuesto a la gestión de seguridad de información. [3]

Luego de lo descrito, a continuación en este capítulo, se explicara la problemática que conlleva la pérdida y daño de la información relevante para la empresa, los

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

objetivos y resultados esperados de esta tesis y el alcance y limitaciones que tendrá el presente proyecto. Además se explicara y dará la justificación de nuestra solución y su viabilidad.

1.2 DEFINICION DE LA PROBLEMÁTICA

Como ya se explico, en los últimos 20 años el uso de las tecnologías, dentro de las organizaciones, ha ido en rápido aumento, ya que permiten optimizar las actividades y procesos de la empresa, además de potenciar las la productividad de las personas. [6]

Con el incremento del uso de dichas tecnologías al interior de estas organizaciones para almacenar, mantener, transmitir y recobrar información, han aumentado también considerablemente la variedad y cantidad de amenazas que podrían afectar la confidencialidad, disponibilidad, auditabilidad e integridad de la información vital para la organización [6], el negocio y los clientes, lo que podría provocar graves pérdidas económicas, y de tiempo para la organización.

En la Ilustración 1-1 se puede apreciar como los activos de información de una organización están rodeados de un ambiente complejo lleno de amenazas que pueden ir desde simples virus de computadora hasta robo de la propiedad intelectual de la empresa.

Ahora, también es un hecho cierto que así como existen especialistas en el mundo de la tecnología, dedicados a desarrollar, por el bien de la comunidad nuevos software que ayudan a mejorar y facilitar la vida de los seres humanos, ya sea en el área de negocios como en el área personal, también existen los llamados “hackers” o piratas cibernéticos, casi siempre jóvenes con avanzados conocimientos de informática que utilizan su inteligencia para robar información de grandes empresas, gobierno y hasta organizaciones sin o con fines de lucro.

Además, el instituto Ponemon también dice que cada filtración de información hace que las compañías pierdan el 3,7% de sus clientes en promedio. Pero ese no es el único costo de la filtración.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

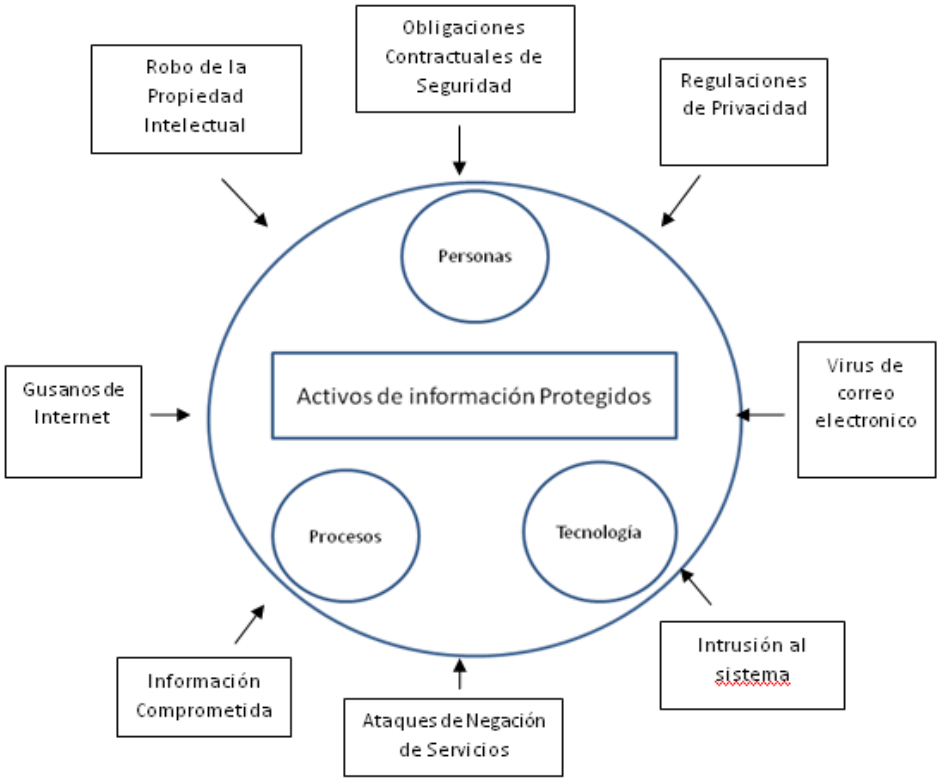


Ilustración 1-1.Activos de Información y sus amenazas

Las compañías deben mejorar sus sistemas y capacitar a su equipo para encontrar y resolver el problema, que no es nada barato. Después del robo, las compañías deben informar a sus clientes que la información está en riesgo, y deben gastar incluso más para prevenir que vuelva a ocurrir [17].

Para el caso del presente proyecto de tesis, se realizó un enfoque en la seguridad de una empresa del rubro de producción y distribución de alimentos de consumo masivo, donde también aplica la necesidad de proteger la información. Por ejemplo, en unos de sus principales procesos que es el de Producción, el cual se divide a su vez en 4 subprocesos que son Planeamiento, Manufactura, Calidad y Bodegas e Inventarios. En estos subprocesos está implicada información de gran importancia para la empresa, como “recetas” de productos, programación de manufactura, sistemas que se usan, tipos de pruebas de calidad de producto, etc., la cual debe estar resguardada correctamente para evitar que dicha información se pierda o caiga en manos indebidas y así garantizar la continuidad de la empresa y el logro los objetivos del negocio.

Además este sistema de gestión de seguridad de información que se diseñó, no solo será útil para el tipo de empresa de producción y distribución de alimentos de

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

consumo masivo, sino también será útil para todos los tipos de empresas de producción que tengan como información relevante a fórmulas de sus productos, programación de producción, planes de producción, recetas, materias primas, estructura de sus productos, etc. Algunos tipos de empresa son por ejemplo una empresa productora de cerámicos, una empresa productora de productos farmacéuticos, una empresa productora de bebidas, etc. que precisamente tienen como información relevante la receta de sus distintos tipos de productos (cerámicos, fármacos, gaseosas), sus planes de producción, Schedule, etc.

Para garantizar la seguridad de esta información, las empresas deben dejar de actuar reactivamente en respuesta a los incidentes y problemas relacionados con la seguridad de información y empezar a realizar un conjunto de acciones como identificar el activo y definir su impacto, luego evaluar cuáles de estos activos puede correr riesgos y por último la alta gerencia deben decidir qué acciones se tomarán para mitigar los riesgos.

Esta importancia de la información crea una necesidad de control y gestión de la seguridad sobre la misma y no solo desde un punto de vista legal en cuanto a datos personales se refiere, sino con carácter general a toda la información manejada por una compañía, convirtiéndose en un complemento importante y que aporta un plus de confianza y compromiso ante clientes o terceros ajenos a la empresa. Como ejemplo de este punto es la cada vez más aceptada e incluso exigida aplicación de normas ISO en la contratación entre empresas a nivel internacional. Este sistema de gestión es de mucha importancia para que una organización pueda sobrevivir al mercado actual.

Para gestionar la seguridad de la información, las organizaciones pueden seguir algunas de las normas o modelos existentes en el mercado, tales como ISO/IEC 27001 e ISO/IEC 27002, RISK IT, COBIT, etc., que establecen determinadas reglas y estándares que sirven de guía para esta gestión.

1.3 OBJETIVO GENERAL DEL PROYECTO DE TESIS

El objetivo general del presente proyecto de fin de carrera es analizar y diseñar un sistema de gestión de seguridad de información, basado en la norma ISO/IEC 27001:2005 para una empresa dedicada a la producción y comercialización de alimentos de consumo masivo.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

1.4 OBJETIVOS ESPECIFICOS DEL PROYECTO DE TESIS

OE1: Inventariar los procesos de negocio, los procesos de tecnologías de información (TI) que dan soporte a los esos proceso de negocio y finalmente los activos relacionados con estos procesos.

OE2: Identificar y analizar los riesgos de seguridad de información de los principales procesos identificados, aplicando la metodología MAGERIT.

OE3: Elaborar el sistema de gestión de seguridad de información (SGSI) en base a la norma ISO/IEC 27001:2005 para el SGSI que se quiere diseñar, y elegir los controles basándose en la norma ISO/IEC 27002.

OE4: Documentar el SGSI de acuerdo a la norma ISO 27001.

1.5 RESULTADOS ESPERADOS DEL PROYECTO DE TESIS

RE1: El inventariado de procesos principales del negocio. Este resultado se verificará con el documento en sí, y con la relación de los procesos, más importantes de la empresa, sobre los que se trabajó. (Relacionado con el OE 1).

RE2: Matriz de riesgos, cuyo propósito es determinar y entender qué procesos son esenciales para la continuidad de las operaciones, calcular su posible impacto y los tiempos máximos tolerables de interrupción así como sus tiempos estimados de recuperación. Para ello se realiza el análisis de riesgos, que puedan impactar en estos procesos, mediante el método *Magerit* (Metodología de Análisis y Gestión de Riesgos de IT) que sirve para realizar los pasos delineados del análisis de riesgos pero siguiendo una serie de pasos determinados y concretados. (Relacionado con el OE2)

RE3: Documento con la declaración de aplicabilidad de la norma ISO 27001 para el SGSI que se quiere diseñar. Se verifica con el documento en sí. (Relacionado con el OE3)

RE4: Documentación obligatoria exigida por la norma ISO 27001 para implantar un SGSI. (Relacionado con el OE4)

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

1.6 ALCANCE Y LIMITACIONES

Este proyecto tiene un alcance y limitaciones determinado que permite acotar el análisis y diseño del SGSI para la empresa productos de alimentos. El alcance y las limitaciones del proyecto se describen a continuación.

1.6.1 Alcance

El alcance del presente proyecto de fin de carrera, abarca el diseño del SGSI, basado en la norma ISO/IEC 27001:2005 y está dirigido a procesos, activos, riesgos, y demás consideraciones, de una empresa de producción y comercialización de productos de consumo masivo. El trabajo cubrirá todos aquellos aspectos a tener en cuenta en relación a estándares, procedimientos, normas y medidas que empleen tecnología que permitan asegurar las principales característica que debe tener la información que son integridad, disponibilidad y confidencialidad en sus estados de proceso, almacenamiento y transmisión y auditabilidad.

El alcance del proyecto abarca solo el proceso considerado principal para el negocio e importante para la continuidad del negocio que tenga con mayor impacto. Este proceso es el de “Producción” que como ya se mencionó anteriormente abarca cuatro subprocesos que son “Planificación de producción”, “Manufactura de producto”, “Calidad de producto” y “Bodegas e Inventarios”. Más adelante, en el Capítulo 2, en la parte del análisis del SGSI se detalla esto procesos.

1.6.2 Limitaciones

Las principales limitaciones del proyecto son:

- Este proyecto de de tesis consistirá solo en el análisis y diseño del SGSI basado en la norma ISO 27001, pero no abarca la parte de la implementación del SGSI dentro de una empresa.
- El proyecto plantea algunos controles, que serán indispensables para proteger los activos de información más importantes de la empresa, pero si cambia alguna regulación a nivel nacional, la cual le exija a la empresa muchos controles extras, el SGSI no podrá abarcar esa necesidad contractual que tendría la organización.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

1.7 METODOS Y PROCEDIMIENTOS

La norma ISO 27001:2005 ha sido desarrollada con el fin de servir como modelo para el establecimiento, implementación, seguimiento y mejora de un SGSI en cualquier tipo de organización basándose en sus propios objetivos y requerimientos de seguridad y usando además, los controles sugeridos en la norma ISO/IEC 27002 [1].

Para este proyecto y para el producto final del mismo, que es la implementación del SGSI, se usara la metodología del ciclo de Deming (Plan-Do-Check-Act), y para el análisis de riesgo se usara la metodología MAGERIT II, las cuales se presentan a continuación dimensionadas al proyecto.

1.7.1 Ciclo de Deaming (Plan-DO-CHECK-OUT)

A continuación en la Tabla 1-1 se muestra en una tabla los aspectos considerados en cada etapa del ciclo de Deaming, para el proyecto y para el SGSI.

ETAPA	ACCIONES	
	SGSI	PROYECTO
PLANEAR	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.	Definir el problema a resolver, la forma en que se buscara resolverlo, definir el objetivo general y objetivos específicos, definir el alcance y las limitaciones que tendrá el proyecto de tesis, realizar la planificación temporal del proyecto y elegir los métodos y procedimientos que se emplearan.
HACER	Implementar y operar la política, controles, procesos y procedimientos SGSI.	Desarrollo del proyecto, documentar y controlar las acciones realizadas, levantar información, implementación del SGSI para el tipo de empresa seleccionada, etc.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

CHEQUEAR	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.	Luego de desarrollado e implementado el SGSI, volver a revisar los datos obtenidos y analizarlos, comparándolos con los objetivos específicos iniciales, para evaluar si se han obtenido los resultado esperados.
ACTUAR	Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoría interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.	Modificar y corregir algunos aspectos errados encontrados en la etapa anterior, con el fin de garantizar que se obtengan los resultados esperados del proyecto, aplicar mejoras y terminar de documentar todo el proyecto.

Tabla 1-1: PDCA para el Proyecto y el SGSI.

Como este proyecto de fin de carrera solo abarca el análisis y diseño del SGSI, solo se tomarán en cuenta las etapas de “Planear” y “Hacer” (Plan – Do) de la metodología, como base el proyecto.

1.7.2 MAGERIT II

Luego para el análisis y administración de riesgos necesario para la implementación del SGSI, se usara la metodología MAGERIT II [3].

MAGERIT II es una metodología para administrar riesgos, que tiene como uno de sus principales objetivos, el ofrecer un método para analizar los riesgos y ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control [3].

El análisis de riesgos propuesto por MAGERIT II es una aproximación metódica que permite determinar el riesgo siguiendo los siguientes pasos:

- Determinar los activos relevantes para la empresa.
- Determinar las amenazas a la que están expuestos aquellos activos.
- Estimar el impacto, definido como el daño sobre el activo, si se llega a concretar la amenaza.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

- Valorar dichos activos en función del coste que supondría para la empresa recuperarse ante un problema de disponibilidad, integridad o confidencialidad de información.
- Valorar las amenazas potenciales.
- Estimar el riesgo.

1.8 JUTIFICACION Y VIABILIDAD

A continuación, se darán algunos puntos claves, que justifican y muestran la viabilidad de la solución que se busca desarrollar en el presente proyecto de tesis para la problemática mencionada anteriormente. Además se

1.8.1 Justificación

Los motivos que justifican por qué el análisis y desarrollo de un SGSI basado en ISO 27001 e ISO 27002, es la solución adecuada para el problema.

- Como ya se mencionó, cuando se habla de información en el ámbito profesional, se refiere a uno de los activos más importantes que manejan las empresas como elemento básico sobre el que fundamentan, realizan y prestan sus servicios. Por ello la gestión de esta información, sea personal, económica, estratégica u organizativa cobra una importancia vital para la consecución de los objetivos marcados y el buen desarrollo del negocio.

  Todas las organizaciones tienen diferentes activos críticos de información, dependiendo del impacto o perjuicio grave que podría tener para la empresa, el que una persona físico o jurídico pueda acceder/obtener/tratar/difundir la misma fraudulentamente o ilícitamente.

  En el caso de una empresa del rubro de producción y comercialización de productos alimenticios de consumo masivo, los activos de información más críticos serian: las marcas de sus productos, información relativa a los productos, clientes, proveedores, personal, método de trabajo, organización, estrategias empresariales, información económica y financiera, etc.

- La expectativa de perdidas anuales (ALE) de una empresa, se basa en la frecuencia y magnitud de probables incidentes de seguridad para esa organización. El ALE teórico para una empresa, si no protege su

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

información, es muy alto, ya que cuando los corporativos son atacados, los costos son enormes y aumentan rápidamente.

Este año, por ejemplo, las compañías estadounidenses gastaran más de 130,000 millones de dólares como resultado de filtraciones de información, según el instituto Ponemon, una organización de investigación de seguridad cibernética. Eso es más del triple de los que las compañías gastaron para combatir filtraciones en el 2006 [16].

Además como se describió en la problemática, el instituto Ponemon dice que cada filtración de información hace que las compañías pierdan el 3,7% de sus clientes en promedio.

El instituto Ponemon también dice que cada filtración de información hace que las compañías pierdan el 3,7% de sus clientes en promedio. Pero ese no es el único costo de la filtración. Las compañías deben mejorar sus sistemas y capacitar a su equipo para encontrar y resolver el problema, que no es nada barato. Después del robo, las compañías deben informar a sus clientes que la información está en riesgo, y deben gastar incluso más para prevenir que vuelva a ocurrir [17].

Las compañías también deben pagar por la limpieza tras el ataque; ese costo suele superar el valor de la información robada. Cada documento robado costó, en promedio, 204 dólares en 2009, 144 de los cuales no estaban directamente relacionados con la información misma [18].

- Uno de los aspectos más importantes es comprender que la información debe ser gestionada, especialmente cuando se trata de proteger redes corporativas.

  La gestión de la información, sea personal, económica, estratégica u organizativa cobra una importancia vital para la consecución de los objetivos marcados y el buen desarrollo del negocio.

  Esta importancia de la información crea una necesidad de control y gestión de la seguridad sobre la misma y no solo desde un punto de vista legal en cuanto a datos personales se refiere, sino con carácter general a toda la información manejada por una compañía, convirtiéndose en un complemento importante y que aporta un componente de confianza y

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

compromiso ante clientes o terceros ajenos a la empresa. Como ejemplo de este punto es la cada vez más aceptada e incluso exigida aplicación de normas ISO en la contratación entre empresas a nivel internacional.

Para eso se tiene un concepto muy importante: Sistema de Gestión de Seguridad de Información (SGSI). Un SGSI implica crear un plan de diseño, implementación, y mantenimiento de una serie de procesos que permitan gestionar de manera eficiente la información, para asegurar la integridad, confidencialidad y disponibilidad de la información. [2]

Muchas organizaciones creen que implementar un SGSI es demasiado esfuerzo, y está solo destinado a grandes corporaciones, lo que a veces termina derivando en un manejo caótico o muy minimalista de la administración de la seguridad. Sin embargo es posible en algunos casos aplicar unos pocos principios, en lugar de un SGSI completo, para conseguir mejoras significativas. Para esto será necesario olvidar las formalidades del cumplimiento de una norma, pero sin dejar de seguir sus lineamientos principales.

Pero desde el punto de vista de la alta gerencia, un SGSI permite obtener una visión global del estado de los sistemas de información sin caer en detalles técnicos, además de poder observar las medidas de seguridad aplicadas y los resultados obtenidos, para poder con todos estos elementos tomar mejores decisiones estratégicas.

En este proyecto de tesis finalmente, se considera la norma ISO 27001, que es la norma más usada para establecer un correcto SGSI, la cual especifica los requisitos necesarios para establecer y para certificar un SGSI; y la norma ISO 27002, la cual describe un código de buenas prácticas para la gestión de la seguridad de la información y los controles recomendables relacionados con la seguridad.

1.8.2 Viabilidad

Aquí se procederá a detallar la viabilidad técnica y económica que tiene el desarrollo del presente proyecto de fin de carrera.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

1.8.2.1 Viabilidad Técnica

Para la realización de este proyecto de tesis, es decir, para el diseño del SGSI se necesitaran una serie de informaciones, que juntas forman una cadena de acción, tal como se muestra a continuación en la Ilustración 1-2:

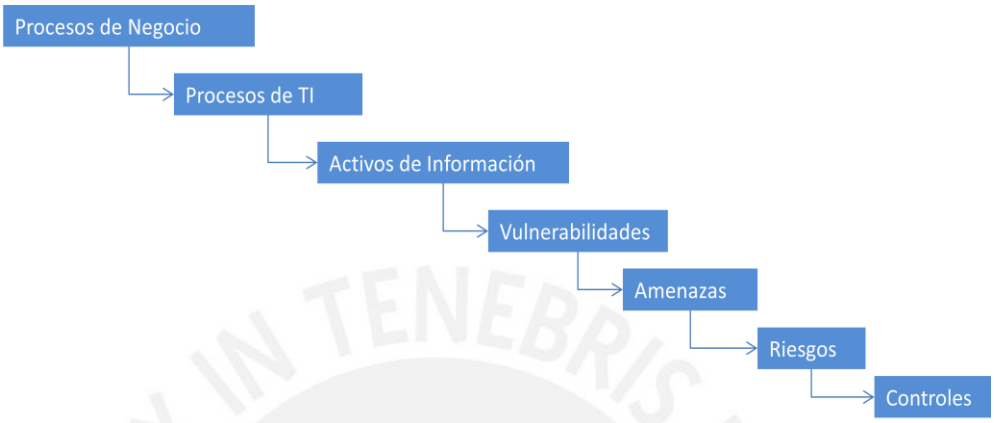


Ilustración 1-2: Escalera de la seguridad de Información

Finalmente con la suma de todos los controles planteados permitirá administrar, y diseñar el SGSI.

1.8.2.2 Viabilidad Económica

- Para el desarrollo de esta tesis, se necesitara adquirir las normas ISO 27001 e ISO 27002. La norma ISO 27001 cuesta $189.00 dólares americanos y la norma ISO 27002 cuesta $158.00 dólares americanos.
- El costo de hora hombre para realizar este proyecto será de S/180.00 incluido IGV.
- Se requerirá comprar el libro “Diseño de un Sistema de Gestión de Seguridad de Información / Óptica ISO 27001:2005. Primera edición.” del autor Alexander G., Alberto. Cuyo costo es de S/60.00 soles.

Por lo tanto luego de los descrito, se llego a la conclusión que con los medios con los que se cuenta, es viable y factible poder desarrollar de manara completa y correcta este proyecto de fin de carrera.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

1.9 MARCO CONCEPTUAL

Hay algunas definiciones importantes relacionadas al tema de Gobierno de TI, seguridad de información y SGSI, que son útiles para una mejor comprensión de este proyecto.

A continuación en este capítulo, se detallara el marco conceptual del tema y se dará a conocer estado del arte actual de la solución planteada.

1.9.1 Información

Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. La información ya sea impresa, almacenada digitalmente o hablada, actualmente es considerada como un activo dentro de las compañías, y que se debe proteger, mediante soportes de muy distintas formas, ya que es de gran importancia. [1]

1.9.2 Activos de Información

Los activos son los recursos que tienen valor o utilidad para la organización, sus operaciones comerciales y su continuidad, necesarios para que la organización funcione y alcance los objetivos que propone su dirección. [3]

En este punto es importante aclarar que es un activo de información en el contexto del ISO 27001:2005. Según el ISO 17799:2005 (Código de Práctica para la Gestión de Seguridad de Información), un activo de información es: [2]

> *"… algo a lo que una organización directamente le asigna un valor y, por lo tanto, la organización debe proteger".*

El ISO 17799:2005 clasifica los activos de información en las categorías siguientes: [2]

- Activos de información (datos, manuales de usuario, etc.).
- Documentos de papel (contratos).[5]
- Activos de software (aplicación, software de sistemas, etc.).
- Activos físicos (computadoras, medios magnéticos, etc.).
- Personal (clientes, personal).
- Imagen de la compañía y reputación.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

- Servicios (comunicaciones, etc.).

1.9.3 Gestión de Riesgos

Normalmente las corporaciones, suelen tener muy poco conocimiento del impacto que pueden tener la pérdida de los activos de información o la imposibilidad para acceder a sus sistemas. [20]

La gestión de riesgo es un enfoque estructurado para manejar la incertidumbre, es decir la posibilidad de que ocurra o no un riesgo, para evitar que ocurran consecuencias no deseadas dado el caso que el riesgo se haga realidad, para ello se pueden llevar a cabo una secuencia de actividades para evaluar el riesgo, mitigar el riesgo y estrategias para manejar el riesgo que incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular de tal forma que las posibles pérdidas y la posibilidad que se haga presente el riesgo se minimicen. [7]

En resumen la Gestión de Riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo.

A continuación se presentan las definiciones de algunos términos importantes que se ven en la gestión de riesgos.

1.9.3.1 Amenazas

En las organizaciones, los activos de información están sujetos a distintas formas de amenazas.

Una amenaza es todo aquello, ya sea físico o lógico que puede causar un incidente no deseado, generando daños materiales o inmateriales a la organización y a sus activos, como la perdida de información, o de su privacidad, o bien un fallo en los equipos físicos. [5]

Las amenazas conviene clasificarlas por su naturaleza, para así facilitar su ubicación. Se tienen seis tipos de amenazas: [2]

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

- Amenazas naturales (inundaciones, tsunamis o maremotos, tornados, huracanes, sismos, tormentas, incendios forestales).
- Amenazas a instalaciones (fuego, explosión, caída de energía, daño de agua, perdida de acceso, fallas mecánicas).
- Amenazas humanas (huelgas, epidemias, materiales peligrosos, problemas de transporte, pérdida de personal clave).
- Amenazas tecnológicas (virus, hacking, pérdida de datos, fallas de hardware, fallas de software, fallas en la red, fallas en las líneas telefónicas).
- Amenazas operacionales (crisis financieras, perdida de suplidores, fallas en equipos, aspectos regulatorios, mala publicidad).
- Amenazas sociales (motines, protestas, sabotaje, vandalismo, bombas, violencia laboral, terrorismo).

Como se puede ver en la Ilustración 1-3, el origen de las amenazas pueden tener distintas fuentes que pueden ser accidentales o deliberados.

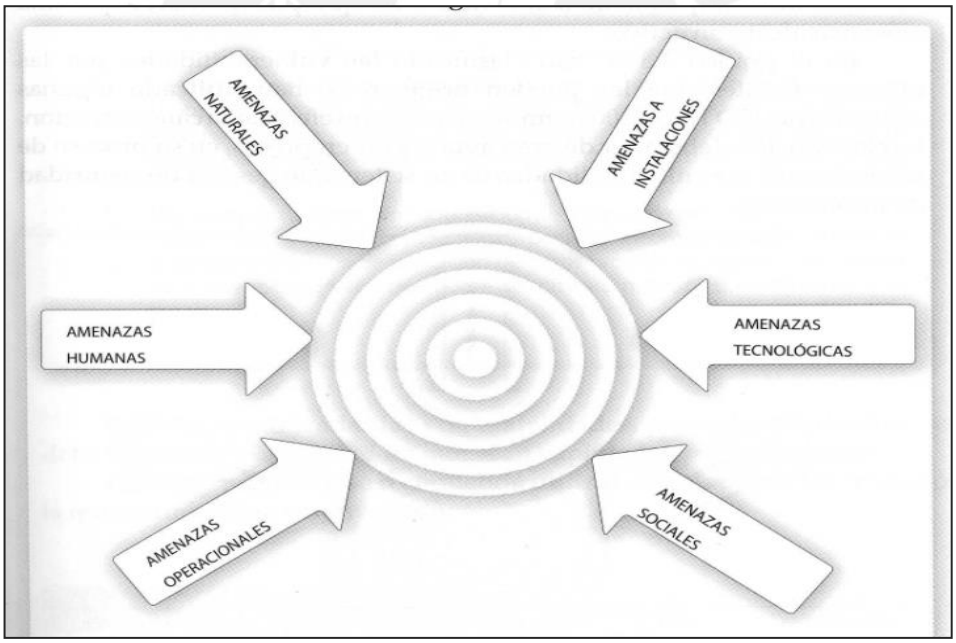


Ilustración 1-3: Tipos de Amenazas a la información. [2]

1.9.3.2 Vulnerabilidades

Las vulnerabilidades son debilidades de seguridad asociadas con los activos de información de una organización. [2]

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

"Es una debilidad en el sistema, aplicación o infraestructura, control o diseño de flujo que puede ser explotada para violar la integridad del sistema" (Peltier, 2001).

"Las vulnerabilidades organizacionales son debilidades en las políticas organizacionales o prácticas que pueden resultar en acciones no autorizadas" (Albert y Dorofee, 2003).

Las vulnerabilidades pueden clasificarse en las siguientes categorías:

- Seguridad de los recursos humanos (falta de entrenamiento en seguridad, carencia de toma de conciencia en seguridad, falta de mecanismos de monitoreo, falta de políticas para el uso correcto de las telecomunicaciones, no eliminar los accesos al término del contrato de trabajo, carencia de procedimiento que asegure la entrega de activos al término del contrato de trabajo, empleados desmotivados).[4]
- Control de acceso (Segregación inapropiada de redes, falta de política sobre escritorio y pantalla limpia, falta de protección al equipo de comunicación móvil, política incorrecta para control de acceso, password sin modificarse). [4]
- Seguridad física y ambiental (control de acceso físico inadecuado a oficinas, salones y edificios, ubicación en áreas sujetas a inundaciones, almacenes desprotegidos, carencia de programas para sustituir equipos, mal cuidado de equipos, susceptibilidad de equipos a variaciones de voltaje). [4]
- Gestión de operaciones y comunicación (complicadas interfaces para usuarios, control de cambio inadecuado, gestión de red inadecuada, carencia de mecanismos que aseguren el envío y recepción de mensajes, carencia de tareas segregadas, carencia de control de copiado, falta de protección en redes públicas de conexión). [4]
- Mantenimiento, desarrollo y adquisición de sistemas de información (protección inapropiada de llaves criptográficas, políticas incompletas para el uso de criptografía, carencia de validación de datos procesados, carencia de ensayos de software, documentación pobre de software, mala selección de ensayos de datos). [4]

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

1.9.3.3 Impacto

El impacto en un activo es la consecuencia sobre éste de la materialización de una amenaza. De forma dinámica, es la diferencia en las estimaciones del estado de seguridad del activo antes y después de la materialización de la amenaza sobre éste. [3]

La Ilustración 1-4 muestra la relación entre impacto y amenaza.

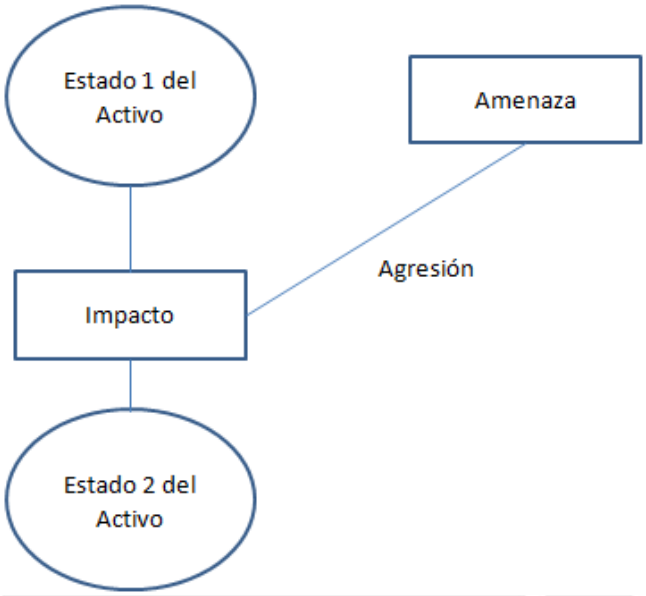


Ilustración 1-4: Relación entre impacto y Amenazas.

1.9.3.4 Riesgos

El riesgo es la posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización.

En el cálculo del riesgo tiene gran influencia la evaluación del impacto, que es un proceso difícil. El nivel del riesgo depende de la vulnerabilidad y del impacto.

El proceso de identificación y evaluación de riesgos –y el de clasificación de activos- permite determinar qué tan expuestos se encuentran los activos de información a ataques por la presencia de vulnerabilidades propias o inherentes a la actividad de la organización.

Existen muchas clasificaciones para tipificar los riesgos, una de ellas es la que aparece en [ISACA, 2011]:

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

- Riesgo inherente: existencia de un error material o significativo sin un control compensatorio.
- Riesgos de control: existencia de un error que no pueda ser detectado por el sistema de controles establecido.
- Riesgos de detección: mal uso de procedimientos de detección de errores por parte de un auditor, que lleven a indicar que no existen errores donde si los haya.
- Riesgos de negocio.
- Otros riesgos generales propios de la naturaleza de la auditoría.

1.9.3.5 Controles

Son las políticas, procedimientos, prácticas y estructuras organizacionales para reducir riesgos y que además proveen cierto grado de certeza de que se alcanzaran los objetivos del negocio.

Existen varias formas de establecer controles sobre riesgos organizacionales. La siguiente es la presentada por [ISACA, 2011]:

- *Disuasivos*: su presencia disuade de la comisión de acciones en contra de alguna política o procedimiento establecido y considerado correcto. Por ejemplo: cámaras de vigilancia.
- *Preventivos*: detectan problemas antes que ocurran por medio de monitoreo constante. Por ejemplo: políticas de contratación.
- *Detectivos*: detectan y reportan los problemas suscitados por errores u omisiones, en el momento en que éstos ocurren. Por ejemplo: Uso de antivirus.
- *Correctivos*: minimizan el impacto de una amenaza ya consumada. Por ejemplo: Planes de contingencia. Propios de cada área administrativa y operativa de las organizaciones.

1.9.4 Gobierno Corporativo

El gobierno corporativo puede ser entendido como: “El proceso mediante el cual, el consejo de administración de una entidad asegura el logro sostenido de sus objetivos, así como la protección de su patrimonio y de los intereses de todos sus *stakeholders* (grupos de interés social), a quienes debe ofrecer transparencia en las prácticas de administración y control de la entidad”. [3]

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

1.9.4.1 Gobierno de TI

El gobierno de TI es parte integral del gobierno corporativo heredando todas sus características generales. Es una estructura de relaciones y proceso que brinda dirección a la empresa con el fin de alcanzar los objetivos de negocio con una adecuada implementación de los procesos de TI en su interior, generando valor a través de TI, logrando gestionar adecuadamente los riesgos de TI. [3][5]

El gobierno de TI es responsabilidad de la junta de directores y gerencia de una organización. [6]

El gobierno de TI nace por la creciente importancia que la tecnología de la información tiene en las organizaciones, tanto por su capacidad de generar valor, como por el potencial impacto de los riesgos relacionados con su empleo. [3]

Los objetivos del gobierno de TI podrían resumirse de la siguiente forma: [3]

- Crear valor para la organización mediante el empleo de tecnología de la información.
- Preservar el valor creado mediante la adecuada administración de riesgos relacionados con la tecnología de información.
- De acuerdo con el marco COBIT, el propósito el gobierno de TI es dirigir las iniciativas y recursos de tecnología de la información para asegurar lo siguiente:
- Que la TI este alineada con la estrategia de la organización y que genere los beneficios que fundamentan su aplicación.
- Que la TI capacite a la organización para aprovechar sus oportunidades y maximizar sus beneficios.
- Que los recursos de TI sean utilizados de manera responsable en beneficio de la organización.
- Que los riesgos relacionados con TI sean administrados de manera adecuada.

En la Ilustración 1-5 se muestra parte del esquema de relaciones dentro de las áreas foco del Gobierno de TI:

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

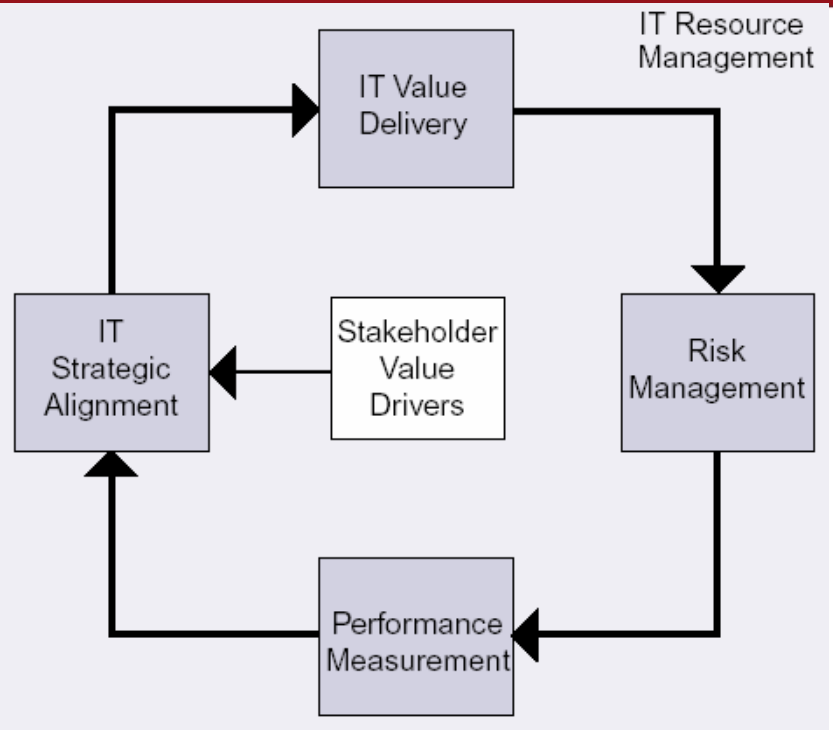


Ilustración 1-5: Esquema de relaciones dentro de las áreas del Gobierno de TI.

En la actualidad, es casi imposible cuestionar la importancia de la información y los sistemas y recursos informáticos que la procesan y distribuyen. Como prueba de esto se tiene a rápida y amplia aceptación que ha tenido el concepto de Gobierno de TI. [3]

Sin embargo, además de los beneficios que trae consigo el uso de las TI, se ha generado también una gran dependencia de las empresas y organizaciones con respecto al empleo de tecnología de la información. Se puede afirmar que existe una relación directa entre e nivel de utilización de las TI y el nivel de dependencia de la empresa. [3]

1.9.4.1.1 Alcance del gobierno del TI

El objetivo principal del gobierno de TI es llevar a cabo proyectos de implementación y uso de tecnologías de información como soporte a las actividades críticas y que le pueda brindar de alguna manera a la Alta dirección la garantía de que la infraestructura tecnológica que tiene el negocio va a permitir lograr los objetivos principales del mismo. [5]

Analizando los aspectos vistos en la Ilustración 1-5 anterior:

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

- **Alineación estratégica:** alinear la tecnología a los objetivos organizacionales, para que respondan como reales soportes.
- **Gestión de riesgos:** el uso de tecnologías de información trae consigo una serie de riesgos a los procesos en donde están brindando soporte. La gestión de riesgos permitirá identificarlos, manejarlos, y reducir el impacto que presentarían sobre los procesos mismos y los activos de información involucrados.
- **Entrega de valor:** optimizar las inversiones de TI.
- **Gestión de recursos:** se debe procurar el uso racional de los recursos asignados a las funciones de TI.

1.9.4.1.2 Beneficios del gobierno del TI

Tener establecido un adecuado gobierno de TI en las organizaciones, que este sincronización con el negocio permite mantener ordenadas las labores de la gerencia de Sistemas / Informática / TI. [5]

ISACA [ISACA, 2010b] señala que los beneficios más destacados de un buen gobierno de TI son:

- Confianza de la alta dirección.
- Sensibilidad a las necesidades del negocio.
- Aseguramiento de los retornos de las inversiones de TI.
- Prestación de servicios más confiables.
- Mayor transparencia en el manejo de gerencia de TI.

1.9.4.2 Seguridad de Información

Está caracterizada por la preservación de los siguientes aspectos: [6]

i. **Confidencialidad:** Asegurando que la información seas accesible solo por aquellos que están autorizados.
ii. **Integridad:** Salvaguardando la exactitud de la información en su procesamiento, así como su modificación autorizada.
iii. **Disponibilidad:** asegurando que los usuarios autorizados tengan acceso a la información y a los activos asociados cuando sea requerido.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

Es importante aclarar una importante diferencia, que La seguridad de TI o Seguridad Informática se ocupa de la salvaguarda de la tecnología y de la información contenida en ellas, mientras que la seguridad de información se ocupa de los riesgos, beneficios y procesos involucrados en la manipulación de la información dentro de la organización, independientemente de cómo sea creada, manejada, transportada o almacenada. [5]

Por otro lado la Seguridad Computacional, es un término más general que abarca una gran área de computación y procesamiento de la información. La seguridad computacional no se limita solo al hardware y software, también le compete el uso adecuado de las instalaciones donde se manejan, es decir, implementar políticas de seguridad que regulen el transito del personal, maquinaria e insumo en la empresa, contemplar medidas de contingencia en caso de catástrofes, etc. [7]

1.9.4.3 Gobierno de la Seguridad de Información

El gobierno de la seguridad de la información es un conjunto de responsabilidades y prácticas que deben ser ejercidas por la alta dirección de las organizaciones para ayudar a dirigir y guiar de forma adecuada, eficiente y responsable todos los aspectos que estén relacionados con todos los activos de información del negocio para así poder lograr cumplir los objetivos estratégicos del negocio.

1.9.4.3.1 Principios básicos para un eficaz gobierno de Seguridad de Información

Algunos principios básicos son: [NCSP, 2009]

- Los directores generales (Alta dirección) deben evaluar, al menos una vez al año, la seguridad de información y los resultados de los programas implantados, para luego reportarlo a la instancia correspondiente.
- La organización como tal, debe actualizar su análisis de riesgos relativo a la seguridad de información con cierta periocidad, revisando que las políticas y procedimientos estén implementado de acuerdo a esas valoraciones de riesgos en aras e proteger los activos de información.
- Las organizaciones y los responsables designados deben desarrollar planes para cubrir aspectos tales como seguridad en redes, relativa al hardware e incluso seguridad en el desarrollo mismo de sistemas de información.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

- Los responsables deben establecer continuos procesos de capacitación y concientización en temas relativos a la seguridad de información.
- Deben estar claramente definidos los procesos y equipos encargados de tomar las acciones correctivas para resolver cualquier incidente de seguridad.
- La organización procurara la aplicación de estándares internacionales y buenas prácticas para medir el desempeño de la seguridad de información.

1.9.4.3.2 Políticas de Seguridad de Información

Son estándares aplicables a todo nivel de la organización, desde la Alta Gerencia, pasando por los usuarios hasta el personal técnicos que velan por el salvaguarda de los activos de información pero buscando mantener un balance adecuado entre el proceso de controlar (costo y esfuerzo para establecer y monitorear controles) y la productividad (los controles no deben complicar la labor de los usuarios de TI). Son documentos de alto nivel que revelan la filosofía corporativa y el pensamiento estratégico de la organización.

1.9.4.3.3 Procedimientos de Seguridad de Información

Son documentos detallados que explican la manera de implementar las políticas de seguridad previamente establecidas. Estos procedimientos declaran los procesos de negocio y los controles integrados de cada uno de ellos, en lo referente a la seguridad de TI; convirtiéndose en una traducción efectiva de las políticas.

1.9.5 Sistema de gestión de seguridad de información (SGSI)

Para empezar, hay algunos pasos que debería seguir una empresa para proteger sus activos de información. Primero se deben identificar los activos de información que tienen un impacto significativo en el negocio, luego hacerles a cada uno un análisis y evaluación de los riesgos y finalmente decidir cuáles son las alternativas adecuadas para tratar el riesgo a implantar para minimizar las posibilidades de que las amenazas puedan causar daño y no penetren a la organización.[2]

Estos pasos que se han descrito son las acciones que un SGSI busca instaurar en una empresa.

El SGSI es una forma sistemática de administrar la información sensible de una institución, para que permanezca segura. Abarca a las personas, los procesos y las

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

tecnologías de información. La forma total de la seguridad de la información, y la integración de diferentes iniciativas de seguridad necesitan ser administradas para que cada elemento sea completamente efectivo. Aquí es donde entra el Sistema de Gestión de Seguridad de la Información que permite coordinar esfuerzos de seguridad con mayor efectividad. [6]

1.9.6 Normas ISO sobre gestión de seguridad de la información

Una norma es un documento cuyo uso es voluntario y que es el fruto del consenso de las partes interesadas y que deben aprobarse por un Organismo de Normalización reconocido. [4]

El ISO es un organismo internacional que se dedica a desarrollar reglas de normalización en diferentes ámbitos, entre ellos la informática. [4]

El IEC es otro organismo que publica normas de estandarización en el campo de la electrónica. [4]

La serie de normas ISO/IEC 27000 se denomina “Requisitos para la especificación de sistemas de gestión de la seguridad de la información (SGSI)”, 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 de la información.
- Valoración de riesgos.
- Controles.

Esta serie de normas comprenden un conjunto de normas relacionadas con la seguridad de la información cuyo objetivo es que una empresa que aplique correctamente estas normas, pueda estar apta para certificar ISO.

En la serie de normas comprenden ISO 27000 los rangos de numeración reservados por ISO van del 27000 al 27019 y del 27030 al 27044.

Entre las normas de la familia ISO 27000, existen las siguientes:

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

1.9.6.1 ISO/ IEC 27000

Este ISO básicamente contiene una visión general de las normas de la serie y un conjunto de definiciones y términos necesarios para comprender y aplicar la serie.

1.9.6.2 ISO/ IEC 27001

Este ISO sustituye a la **ISO/ IEC 17799-1**, abarca un conjunto de normas relacionadas con la seguridad informática. Se basa en la norma **BS 7799-2** de British Estándar, otro organismo de normalización.

Esta norma es la principal de la serie, y según ella la seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en el tratamiento de la información.

Esta norma tiene como finalidad proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de seguridad de información (SGSI). [8]

La norma ISO/IEC 17799 proporciona un lineamiento de implementación que se puede utilizar cuando se van a diseñar los controles de seguridad.

El SGSI debe ser dinámico para adaptarse a las nuevas necesidades y objetivos de la organización, así como nuevos requerimientos de seguridad según la naturaleza de los procesos, el tamaño y estructura de la organización. [8]

La norma ISO/ IEC 27001:2005 promueve la adopción de un enfoque del proceso para la gestión de seguridad de la información, es decir el manejo de varias actividades interrelacionadas para transformar entradas (inputs) en resultados (outputs). [8]

Esta norma está alineada con las normas ISO/ IEC 9001:2000 e ISO/ IEC 14001:2004 y se aplica a todos los tipos de organizaciones, grande o pequeña y de cualquier parte del mundo y está diseñada para que el SGSI asegure la selección adecuada y proporcione los controles de seguridad que protejan los activos de información y den confianza a las partes interesadas. La norma es particularmente interesante si la protección de la información es crítica, como en finanzas, sanidad sector público y tecnología de la información (TI).

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

ISO/ IEC /IEC 27001 también es muy eficaz para organizaciones que gestionan la información por encargo de otros, por ejemplo, empresas de subcontratación de TI. Puede utilizarse para garantizar a los clientes que su información está protegida.

1.9.6.3 ISO/ IEC 27002

Esta norma se corresponde con la ISO/ IEC 17799, y que describe un código de buenas prácticas para la gestión de la seguridad de la información y los controles recomendables relacionados con la seguridad.

Se debe tener en cuenta que la norma ISO/ IEC 27002 es una guía para conocer que se puede hacer para mejorar la seguridad de la información, expone una serie de apartados a tratar en relación a la seguridad, los objetivos de seguridad a perseguir, una serie de consideraciones (controles) a tener en cuenta para cada objetivo y un conjunto de sugerencias para cada uno de estos controles; mientras que en la norma ISO/ IEC 27001 se habla de los controles de forma residual, no forma parte del cuerpo principal de la norma, lo más importante en esta norma es la "gestión de la seguridad", en forma de Sistema de Gestión. [9]

1.9.6.4 ISO/ IEC 27003

Esta norma contiene básicamente una guía para el diseño e implementación exitosa de un SGSI de acuerdo con el ISO/IEC 27001:2005.

Aquí se describe el proceso de especificación y diseño del SGSI desde el inicio hasta la elaboración de planes de implementación, describe el proceso de obtener la aprobación de la gestión para implementar un SGSI, define un proyecto para implementar un SGSI, y proporciona orientación sobre como planificar el proyecto de SGSI, lo que resulta en un plan de ejecución final del proyecto SGSI. [10]

1.9.6.5 ISO/ IEC 27004

La norma internacional ISO/IEC 27004:2009 proporciona orientación sobre el desarrollo y usos de las medidas y la medición a fin de evaluar la eficacia de un SGSI y los controles o grupos de controles, tal como se especifica en la norma ISO/IEC 27001.

Esto incluiría la política, la gestión de información de riesgos de seguridad, objetivos de control, controles, procesos y procedimientos, y apoyar el proceso de su

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

revisión, lo que ayuda a determinar si alguno de los procesos o los controles del SGSI debe ser cambiado o mejorado. Hay que tener en cuenta que ninguna medida de control puede garantizar una seguridad total. La aplicación de este enfoque constituye un Programa de Medición de Seguridad de la Información.

1.9.6.6 ISO/ IEC 27005

La norma ISO/IEC 27005:2008 es una guía para la gestión de riesgos de seguridad de la información, de acuerdo con los principios ya definidos en otras normas de la serie 27000.

Sustituye (y actualiza) las partes 3 y 4 de la norma ISO/ IEC TR 13335 (Técnicas para la gestión de la seguridad IT y Selección de salvaguardas, respectivamente) y se convierte en la guía principal para el desarrollo de las actividades de análisis y tratamiento de riesgos en el contexto de un SGSI. [12]

Constituye, por tanto, una ampliación del apartado 4.2.1 de la norma ISO/ IEC 27001, en el que se presenta la gestión de riesgos como la piedra angular de un SGSI, pero sin prever una metodología específica para ello. [12]

Para un mejor entendimiento de esta norma es necesario conocer las normas ISO/IEC 27001 y la norma ISO/IEC 27002.

1.9.6.7 ISO/ IEC 27006

El ISO/IEC 27006:2007 es una norma internacional que especifica los requisitos y proporciona orientación para organismos que presten servicios de auditoría y certificación de un sistema de gestión de seguridad (SGSI), además de los requisitos que figuran dentro de la ISO / IEC 17021 e ISO / IEC 27001. [13]

1.9.6.8 ISO/ IEC 27007

El ISO/IEC 27007:2011 es un estándar internacional que proporciona orientación sobre la gestión de un programa de auditoría de un SGSI, sobre la realización de las auditorías, y en la capacidad de los auditores, además de las orientaciones contenidas en la norma ISO/ IEC 19001. [14]

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

Esta norma internacional es aplicable a aquellos que necesitan comprender o realizar auditorías internas o externas de un SGSI o para administrar un programa de auditoría de SGSI.

1.9.6.9 ISO/ IEC 27008

El ISO/IEC TR 27008:2011 (E) es un informe técnico que proporciona una guía en la revisión de la implementación y operación de los controles, incluyendo la comprobación de la conformidad técnica de los controles de los sistemas de información, en conformidad con los estándares de seguridad de información establecidos en una organización. [15]

Este informe técnico se puede aplicar a organizaciones de todo tipo y tamaño, ya sean empresas públicas o privadas, entidades gubernamentales y organizaciones sin fines de lucro.

Este informe técnico no está diseñado para la gestión de las auditorias de sistemas.

1.10 REVISION DEL ESTADO DEL ARTE

Existen varias normas internacionales que rigen las condiciones en el manejo seguro de información y la importancia de aplicar un SGSI en las organizaciones.

Las principales y más usadas son las que pertenecen a la familia de la ISO/ IEC 27000, las cuales describimos al final del marco teórico del presente documento.

Ahora entraremos con más detalle en la principal norma de esta familia, la ISO/IEC 27001:2005, ya que esta norma se puede aplicar a cualquier tipo de organización, sin importar su tamaño ni actividad principal, por lo tanto nos serviría como guía para poder desarrollar un SGSI para una empresa de producción de alimentos de consumo masivo, que es el objetivo de este proyecto de fin de carrera.

1.10.1 ISO/IEC 27001:2005

El Origen de esta norma es británico, recién en octubre del año 2005, la Organización Internacional para la Normalización (ISO) la oficializó como norma.

A la fecha, existen dos documentos utilizados para implantar un SGSI en las organizaciones:

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

- **ISO/IEC 17799:2005**, "Código de práctica de Seguridad en la Gestión de la información". Este modelo da recomendaciones para buenas prácticas. No puede utilizarse para la certificación. [2]
- **ISO/IEC 27001:2005**, "Especificaciones para la Gestión de Sistema de Seguridad de Información". Este modelo es el que permite implantar un SGSI en las empresas y se utiliza para la certificación. [2]

El ISO/ IEC 27001:2005 es el único estándar aceptado internacionalmente para la gestión de la seguridad de la información, aplica a todo tipo de organizaciones, sin importar el tamaño o su actividad.

Este estándar internacional ha sido desarrollado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la información.

1.10.1.1 Alcance del Modelo

Según el estándar, el propósito del modelo, es a través de sus controles de seguridad, reducir las posibilidades de que los activos de información sean afectados por amenazas externas o internas.

1.10.1.2 Aplicación

El estándar indica que el modelo se ha creado para ser aplicable a toda clase de organización, sin importar su tipo, el tamaño y la naturaleza del negocio.

El estándar indica también que si algunos de sus requerimientos no pueden ser aplicados debido al tipo de organización, se puede considerar el requerimiento para su exclusión.

Para que estas exclusiones sean validas, no podrán afectar la capacidad y/o la responsabilidad de la organización a fin de proporcionar seguridad en la información que satisfaga los requerimientos de seguridad determinados por la evaluación de riesgos. [2]

1.10.1.3 Naturaleza del Estándar

El estándar sigue un enfoque de procesos basado en el ciclo Deming del célebre Plan-Do-Check-Act.

Tesis publicada con autorización del autor
No olvide citar esta tesis

El modelo está basado en un enfoque racional para su desempeño y su perfeccionamiento en el tiempo. Primero se exige que el modelo siga una serie de prerrequisitos para que se establezca, a través de la fase denominada “plan”. Luego de establecido el modelo se implementa y opera, siguiendo las lineamientos de la fase “do”. Luego que el modelo se ha implantado y está funcionando, se debe monitorear y revisar durante la fase “Check”.

Por último, con lo observado en la fase “Do” se procede a “actuar” y tomar los correctivos necesarios.

En la Ilustración 1-6 se presenta lo que se ha explicado:

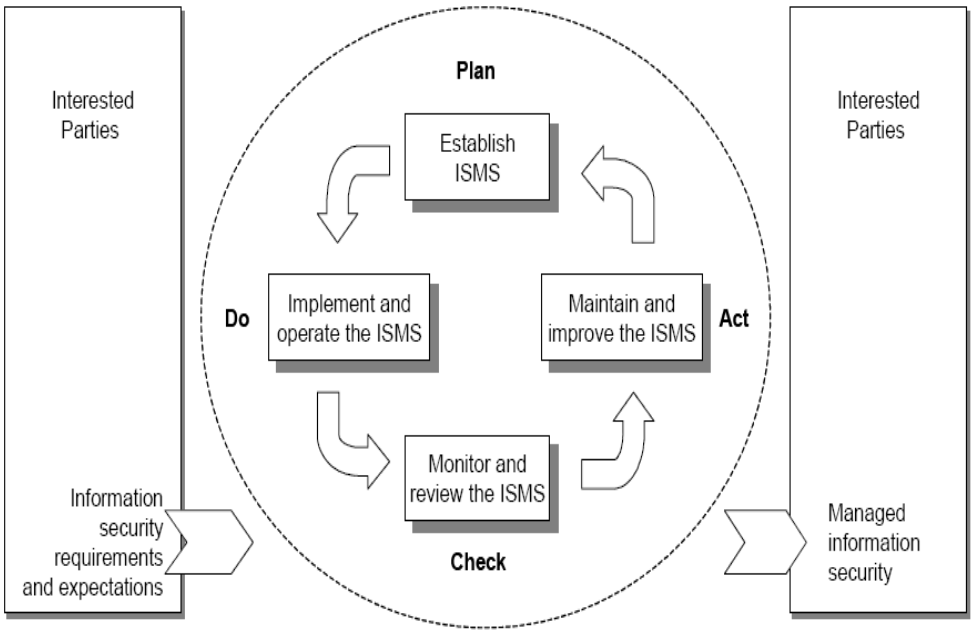


Ilustración 1-6: Diagrama de fases del PDCA. [2]

El proceso de certificación es la generación de un informe firmado por parte de un tercero (ajeno a la organización) que define que, de acuerdo con su criterio personal, dicha organización cumple o no cumple con los requerimientos establecidos en la normativa. [15]

Una certificación es importante para que una organización pueda mostrar al mercado que cuenta con un adecuado sistema de gestión de la seguridad de información. Una empresa certificada no implica que ya no tenga riesgos de

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

seguridad de la información, sino que tienen un adecuado sistema de gestión de dichos riesgos y proceso de mejora continua. [15]

Evidentemente, el paso previo a intentar la certificación es la implantación en la organización del sistema de gestión de seguridad de la información según ISO/ IEC 27001. Este sistema deberá tener un historial de funcionamiento demostrable de al menos tres meses antes de solicitar el proceso formal de auditoría para su primera certificación.

ISO/ IEC 27001 exige que el SGSI contemple los siguientes puntos:

- Implicación de la Dirección.
- Alcance del SGSI y política de seguridad.
- Inventario de todos los activos de información.
- Metodología de evaluación del riesgo.
- Identificación de amenazas, vulnerabilidades e impactos.
- Análisis y evaluación de riesgos.
- Selección de controles para el tratamiento de riesgos.
- Aprobación por parte de la dirección del riesgo residual.
- Declaración de aplicabilidad.
- Plan de tratamiento de riesgos.
- Implementación de controles, documentación de políticas, procedimientos e instrucciones de trabajo.
- Definición de un método de medida de la eficacia de los controles y puesta en marcha del mismo.
- Formación y concienciación en lo relativo a seguridad de la información a todo el personal.
- Monitorización constante y registro de todas las incidencias.
- Realización de auditorías internas.
- Evaluación de riesgos periódica, revisión del nivel de riesgo residual, del propio SGSI y de su alcance.
- Mejora continua del SGSI.

Una vez implantado el SGSI en la organización, y con un historial demostrable de al menos 3 meses, se puede pasar a la fase de auditoría y certificación, que se muestra en la ilustración 1-7 y se desarrolla de la siguiente forma:

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

- Solicitud de la auditoría por parte del interesado a la entidad de certificación y toma de datos por parte de la misma.
- Respuesta en forma de oferta por parte de la entidad certificadora.
- Compromiso.
- Designación de auditores, determinación de fechas y establecimiento conjunto del plan de auditoría.
- Pre-auditoría: opcionalmente, puede realizarse una auditoría previa que aporte información sobre la situación actual y oriente mejor sobre las posibilidades de superar la auditoría real.
- Fase 1 de la auditoría: no necesariamente tiene que ser in situ, puesto que se trata del análisis de la documentación por parte del Auditor Jefe y la preparación del informe de la documentación básica del SGSI del cliente, destacando los posibles incumplimientos de la norma que se verificarán en la Fase 2. Este informe se envía junto al plan de auditoría al cliente. El periodo máximo entre la Fase 1 y Fase 2 es de 6 meses.
- Fase 2 de la auditoría: es la fase de detalle de la auditoría, en la que se revisan in situ las políticas, la implantación de los controles de seguridad y la eficacia del sistema en su conjunto. Se inicia con una reunión de apertura donde se revisa el objeto, alcance, el proceso, el personal, instalaciones y recursos necesarios, así como posibles cambios de última hora. Se realiza una revisión de las exclusiones según la Declaración de Aplicabilidad (documento SOA), de los hallazgos de la Fase 1, de la implantación de políticas, procedimientos y controles y de todos aquellos puntos que el auditor considere de interés. Finaliza con una reunión de cierre en la que se presenta el informe de auditoría.
- Certificación: en el caso de que se descubran durante la auditoría no conformidades graves, la organización deberá implantar acciones correctivas; una vez verificada dicha implantación o, directamente, en el caso de no haberse presentado no conformidades, el auditor podrá emitir un informe favorable y el SGSI de organización será certificado según ISO/ IEC 27001.
- Auditoría de seguimiento: semestral o, al menos, anualmente, debe realizarse una auditoría de mantenimiento; esta auditoría se centra, generalmente, en partes del sistema, dada su menor duración, y tiene como objetivo comprobar el uso del SGSI y fomentar y verificar la mejora continua.

Tesis publicada con autorización del autor
No olvide citar esta tesis

- Auditoría de re-certificación: cada tres años, es necesario superar una auditoría de certificación formal completa como la descrita.

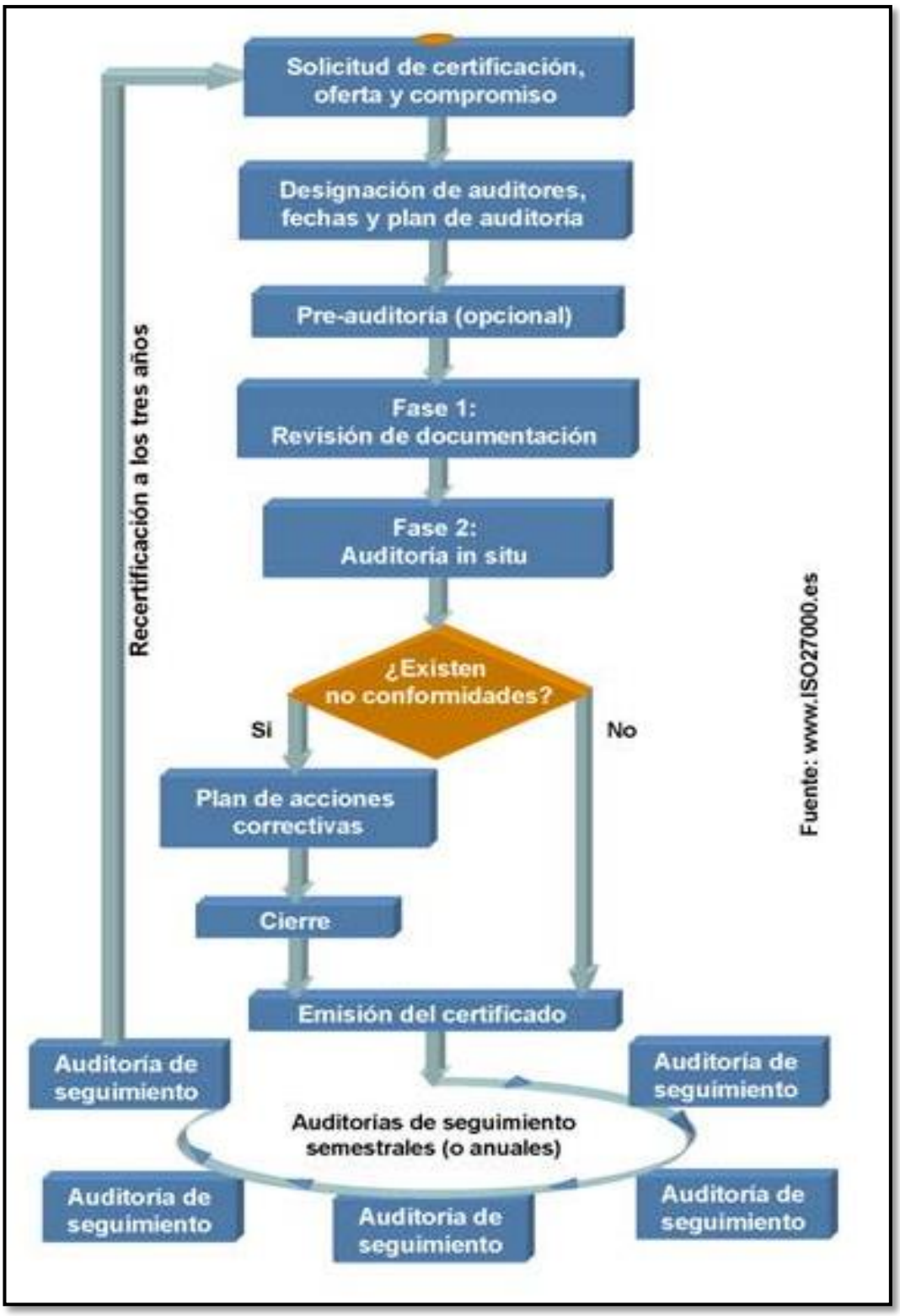


Ilustración 1-7: Proceso de auditoría de un SGSI. [15]

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

1.10.2 Empresas certificadas en la norma ISO/IEC 27001

En la actualidad existen a nivel mundial aproximadamente, 7686 empresas certificadas en la norma ISO/IEC 27001, como se muestra en la tabla.

Como se puede ver en la tabla 1-2, el país con mayor cantidad de empresas certificadas es **Japón con 4004**, seguido muy de lejos por la UK, India y China con 536, 527 y 507 certificaciones respectivamente.

Japan	4004	Croatia	21	Gibraltar	3
UK	536	Slovenia	20	Macau	3
India	527	Bulgaria	18	Qatar	3
China	507	Iran	18	Albania	2
Taiwan	456	Philippines	15	Argentina	2
Germany	202	Pakistan	14	Bosnia Herzegovina	2
Korea	106	Saudi Arabia	14	Cyprus	2
Czech Republic	110	Vietnam	14	Isle of Man	2
USA	104	Iceland	13	Kazakhstan	2
Italy	81	Indonesia	13	Luxembourg	2
Spain	75	Colombia	11	Macedonia	2
Hungary	70	Kuwait	11	Malta	2
Poland	62	Norway	10	Ukraine	2
Malaysia	58	Portugal	10	Mauritius	2
Thailand	48	Sweden	10	Armenia	1
Austria	44	Canada	9	Bangladesh	1
Ireland	44	Russian Federation	9	Belarus	1
Romania	35	Switzerland	9	Denmark	1
Hong Kong	32	Bahrain	8	Ecuador	1
Greece	31	Egypt	5	Jersey	1
Australia	29	Oman	5	Kyrgyzstan	1
Singapore	29	Peru	5	Lebanon	1
Mexico	27	Sri Lanka	5	Moldova	1
France	26	Dominican Republic	4	New Zealand	1
Slovakia	26	Lithuania	4	Sudan	1
Turkey	26	Morocco	4	Uruguay	1
Brazil	24	South Africa	4	Yemen	1
UAE	20	Belgium	3		
Netherlands	22	Chile	3	Total	7686

Tabla 1-2: Número de empresas certificadas en ISO/ IEC 27001 [16]

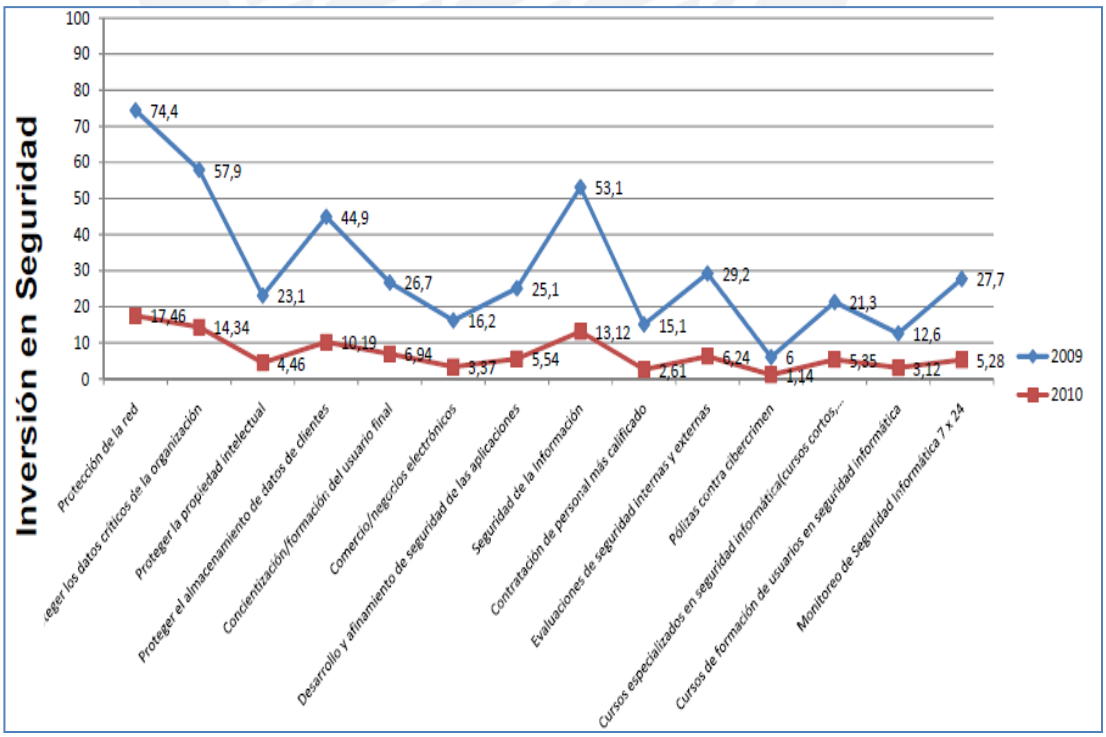
Tesis publicada con autorización del autor
No olvide citar esta tesis

Se puede ver también que en el **Perú** solo hay **5 empresas** que están certificadas en esta norma a través de IRCA, las cuales se muestran en la Tabla 1-3 siguiente. Adicionalmente, la Oficina de Normalización Previsional **ONP** también ha obtenido recientemente la certificación, constituyéndose en la primera institución del Estatal Peruana en alcanzarla.

Name of the Organization	Country	Certificate Number	Certification Body	Standard BS 7799-2:2002 or ISO/IEC 27001:2005
GMD	Peru	SAC 0705104	LRQA	ISO/IEC 27001:2005
Hochschild Minning PLC	Peru	IS 525891		ISO/IEC 27001:2005
Telefonica del Peru	Peru	179684	Bureau Veritas Certification	ISO/IEC 27001:2005
Telefonica Empresas	Peru	179684	Bureau Veritas Certification	ISO/IEC 27001:2005
TELEFONICA GESTION DE SERVICIOS COMPARTIDOS PERU S.A.C.	Peru	GB10/79313	SGS United Kingdom Ltd	ISO/IEC 27001:2005

Tabla 1-3: Número de empresas en el Perú certificados en ISO/ IEC 27001 [16]

Además según la II encuesta Latinoamericana de seguridad de la información (ACIS 2010) que se llevo a cabo en el 2010 se obtuvo como resultado que las empresas estaban invirtiendo en seguridad de información de manera más equitativa con respecto a todas los tópicos de seguridad que está presente dentro de la organización, como se muestra en la Ilustración 1-8:



Tesis publicada con autorización del autor
No olvide citar esta tesis

Ilustración 1-8 Inversiones en Seguridad de Información

Además también se obtuvo como resultado que en el año 2010 estaban aumentando las empresas que tenían sus políticas de seguridad formales, escritas, documentadas e informadas a todo el personal, pero que aún habían muchas que no tenían siquiera una política de seguridad documentada, como muestra el siguiente Ilustración 1-9.

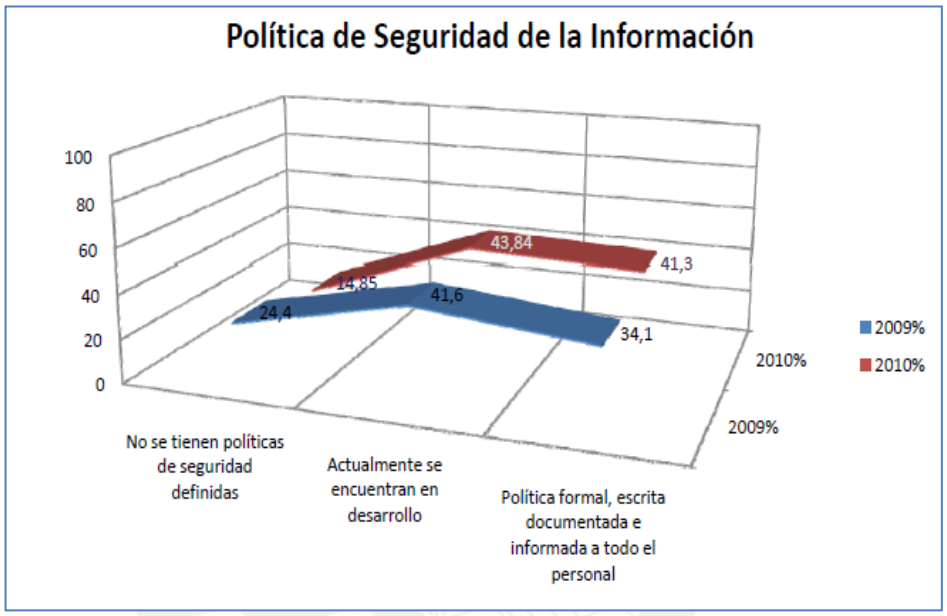


Ilustración 1-9 Política de Seguridad de la Información por Empresa

Por último en este congreso se obtuvo como resultado también que aún seguían predominando en el mercado, empresas y personas que no tenían ningún tipo de certificación en seguridad de información, como muestra la Ilustración 1-8:

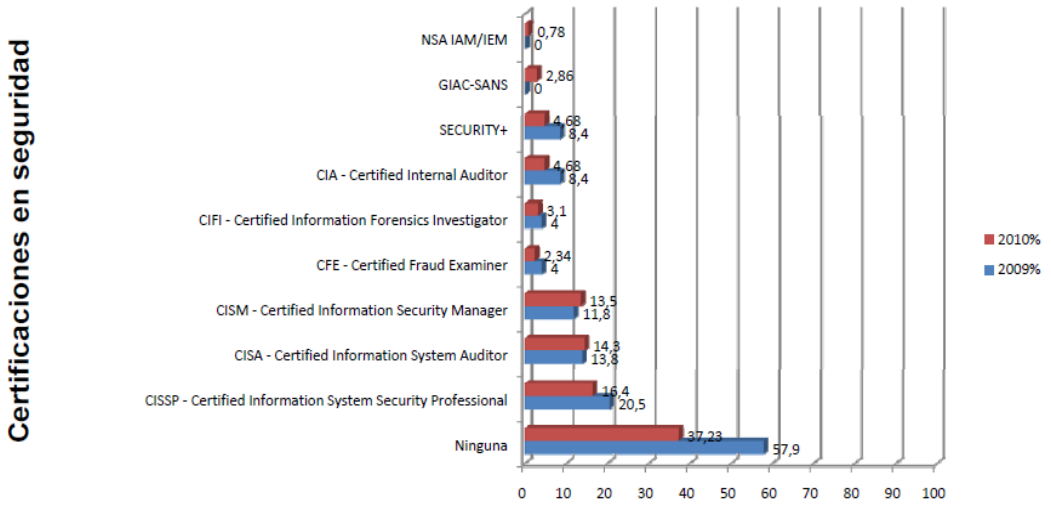


Ilustración 1-10 Certificaciones de Seguridad por Empresa

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

Las principales conclusiones de este congreso fueron:

- Latinoamérica sigue una tendencia de la inversión en seguridad concentrada en temas perimetrales, las redes y sus componentes, así como la protección de datos críticos.
- El poco entendimiento de la seguridad de la información y la falta de apoyo directivo, no pueden ser excusas para no avanzar en el desarrollo de un sistema de gestión de seguridad.
- Si bien están tomando fuerza las unidades especializadas en delito informático en Latinoamérica, es necesario continuar desarrollando esfuerzos conjuntos entre la academia, el gobierno, las organizaciones y la industria, para mostrarles a los intrusos que estamos preparados para enfrentarlos.

1.11 DISCUSION SOBRE LOS RESULTADOS DEL ESTADO DEL ARTE

Como se puede apreciar en las tablas mostradas en las figuras 3.1 y 32, en la actualidad no hay empresas en el país del rubro de producción de alimentos de consumo masivo que estén certificadas en la norma ISO/IEC 27001:2005, y por ende no cuenta con un correcto SGSI implantado.

Es por eso que el motivo de este proyecto de fin de carrera, busca analizar y diseñar un SGSI adecuado, para que se pueda implementar en una empresa del rubro indicado, adecuándose a las necesidades y características de la información de este tipo de organizaciones.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

CAPÍTULO 2 ÁNALISIS DEL SGSI.

2.1 ALCANCE DEL SGSI

Para poder definir el alcance de un SGSI se deben identificar dentro de los procesos con los que cuenta la empresa aquellos considerados como "*core*" para el negocio y delimitar así el SGSI en base a ellos[1]. Una vez identificados, deben definirse los servicios de TI y activos de información involucrados en el soporte a dichos procesos para luego realizar el correspondiente análisis de riesgos.

Los procesos críticos son aquellos que proporcionan el mayor valor a la empresa; es decir, son la parte principal del negocio. Son procesos que de no existir o no funcionar con una regularidad controlada, la empresa no podría alcanzar sus metas y sus objetivos. Por ende, la protección y continuidad de estos procesos es fundamental para cualquier organización.

[1] Algunos especialistas recomiendan a las empresas que recién comienzan a tomar en serio el tema de la seguridad y desea establecer un SGSI, que consideren uno de los procesos críticos de negocios y no la totalidad. Posteriormente y como parte de la mejora continua exigida por la metodología PDCA aplicable a dichos sistemas, se puede ir incorporando al resto de procesos core.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

En el presente proyecto de tesis, para identificar el proceso crítico del negocio se tuvo que realizar un levantamiento de información que permita documentar de forma adecuada al *proceso de producción* y sus subprocesos involucrados debido a que —en el caso de las empresas de producción y comercialización de productos alimenticios de consumo masivo— ser el más importante. .

Este proceso de que abarca cuatro subprocesos a seguir:

- Planificación de Producción.
- Proceso de manufactura.
- Calidad de producto.
- Bodegas e inventarios

2.1.1 Descripción del proceso de Producción

El proceso de producción es un conjunto de acciones, esfuerzos de todos los servicios y ocupaciones profesionales que se encuentran relacionadas con el fin de transformar ciertos elementos, incrementar su valor y así obtener un producto final deseado. [21]

En el caso de la empresa en estudio, las entradas que se van a transformar serían las materias primas como harina, trigo, azúcar, químicos, etc. Y el producto final serial el alimento empaquetado que irá destinado a la venta.

Para la obtención de los productos finales serán necesarias gran cantidad de operaciones individuales, que en conjunto completan todo el flujo de proceso hasta obtener el resultado esperado. Para apoyar cada una de estas operaciones es necesaria la participación de varios tipos de tecnología, tanto software como hardware. El proceso de producción abarca desde el planeamiento de la producción hasta el almacenaje e inventario de los productos. A continuación se muestra el flujo completo de este proceso:

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

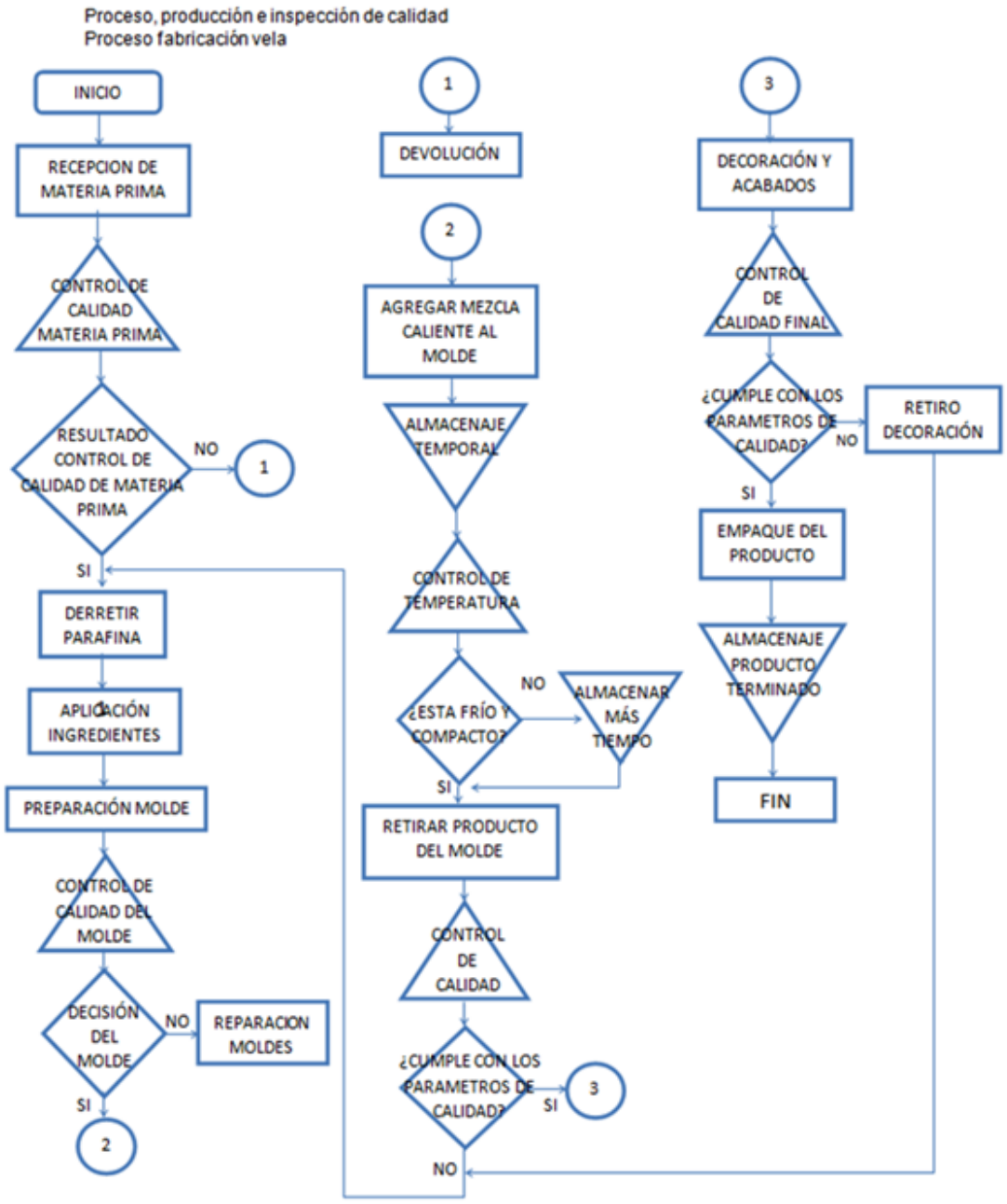


Ilustración 2-1: Flujo completo de Proceso de Producción

2.2 OBJETIVO GENERAL DEL SGSI

Garantizar la seguridad y continuidad de los activos de información críticos que participan en el proceso de producción y sus subprocesos (planeamiento de la producción, calidad, producción, bodegas e inventarios) de la empresa productora de alimentos, sobre la base del análisis de riesgos que haya llevado a cabo la organización.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

2.3 OBJETIVOS ESPECIFICOS DEL SGSI

Los siguientes son los objetivos del sistema de gestión de seguridad de información:

- Garantizar una adecuada clasificación de la información relevante que se maneja en el proceso de producción de la empresa, ofreciendo guías para su clasificación y análisis.
- Realizar el análisis y la gestión de los riesgos de los activos involucrados en el proceso de producción y sus subprocesos.
- Definir los controles que garanticen una adecuada seguridad física y ambiental de los activos de información más relevantes que participan en el proceso de producción, mediante el aseguramiento del perímetro en donde se encuentran alojados los activos y según los planteamientos del anexo A de la ISO/ IEC 27001 (ISO/ IEC 27002).
- Definir los controles que permitan garantizar una adecuada gestión de las comunicaciones y operaciones relacionadas al proceso de producción siguiendo los planteamientos del anexo A de la ISO/ IEC 27001 (ISO/ IEC 27002).
- Definir los controles que permitan garantizar una adecuada gestión de cambios, seguridad de redes, segregación de funcionalidades, gestión de servicios brindados por terceros, intercambio de información interna o externa.
- Elaborar toda la documentación exigida por la norma ISO/ IEC 27001 para el SGSI entre las que destacan: Alcance del SGSI, políticas del SGSI, Metodología empleada para evaluar el riesgo, Informe del análisis de riesgos, plan de tratamiento d riesgos, procedimientos, declaración de aplicabilidad.

2.4 METODOLOGÍA

La parte más importante para el diseño del SGSI, es el análisis y gestión de riesgos de los activos de información que están involucrados dentro el proceso o procesos que abarca el alcance del SGSI.

En este caso, para realizar el análisis de riesgos de los procesos que abarco el alcance del SGSI, se uso como metodología base a MAGERIT II.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

MAGERIT II es una metodología de análisis y gestión de riesgos, la cual permite llevar a cabo:

- El análisis de riesgos de cualquier tipo de sistema de información o de sus elementos, conjuntando en un índice único (el “riesgo”) las estimaciones de sus vulnerabilidades ante las amenazas y del impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización. [3]
- La gestión de los riesgos, basada en los resultados obtenidos en el análisis anterior, seleccionando las medidas o “salvaguardas” (controles) de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles prejuicios. [3]

Esta metodología propone para el análisis de riesgos las 4 etapas siguientes:

- La etapa 1, Planificación del análisis y gestión de riesgos, establece las consideraciones necesarias para arrancar el proyecto de análisis y gestión de riesgos.
- La etapa 2, Análisis de riesgos, permite identificar y valorar las entidades que intervienen en el riesgo.
- La etapa 3, Gestión de riesgos, permite identificar las funciones o servicios de salvaguarda reductores del riesgo detectado.
- La etapa 4, Selección de salvaguardas, permite seleccionar los mecanismos de salvaguarda que hay que implementar.

El análisis de riesgos de este proyecto abarco las etapas 2, 3 y 4. La etapa 1 fue desarrollada en cierta manera en el capítulo 1 de este proyecto.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

CAPÍTULO 3 DISEÑO DEL SGSI.

Para realizar el diseño del SGSI, se realizó primero el análisis y gestión de riesgos del los activos que están involucrados en los procesos de la empresa.

Luego de este análisis se redactó la declaración de aplicabilidad (SOA, Statement of Applicability) donde se detallo los controles relevantes y aplicables al alcance del SGSI que se está diseñando en este proyecto, en función de las conclusiones obtenidas de proceso de evaluación y gestión de riesgos. Con el análisis de la aplicabilidad terminado se realizó el planteamiento de salvaguardas (controles) para cada riesgo identificado en los activos de la empresa, abarcando solo los controles especificados en el SOA.

Para finalizar se plantearon los planes de implementación de los controles seleccionados para cada uno de los riesgos identificados, y además se redactaron las políticas y procedimientos más relevantes para el SGSI.

3.1 ANÁLISIS Y GESTIÓN DE RIESGOS

El análisis y gestión de riesgos es la base de la planificación de los proceso de auditoría, para determinar las vulnerabilidades de los activos de información de las

Tesis publicada con autorización del autor
No olvide citar esta tesis

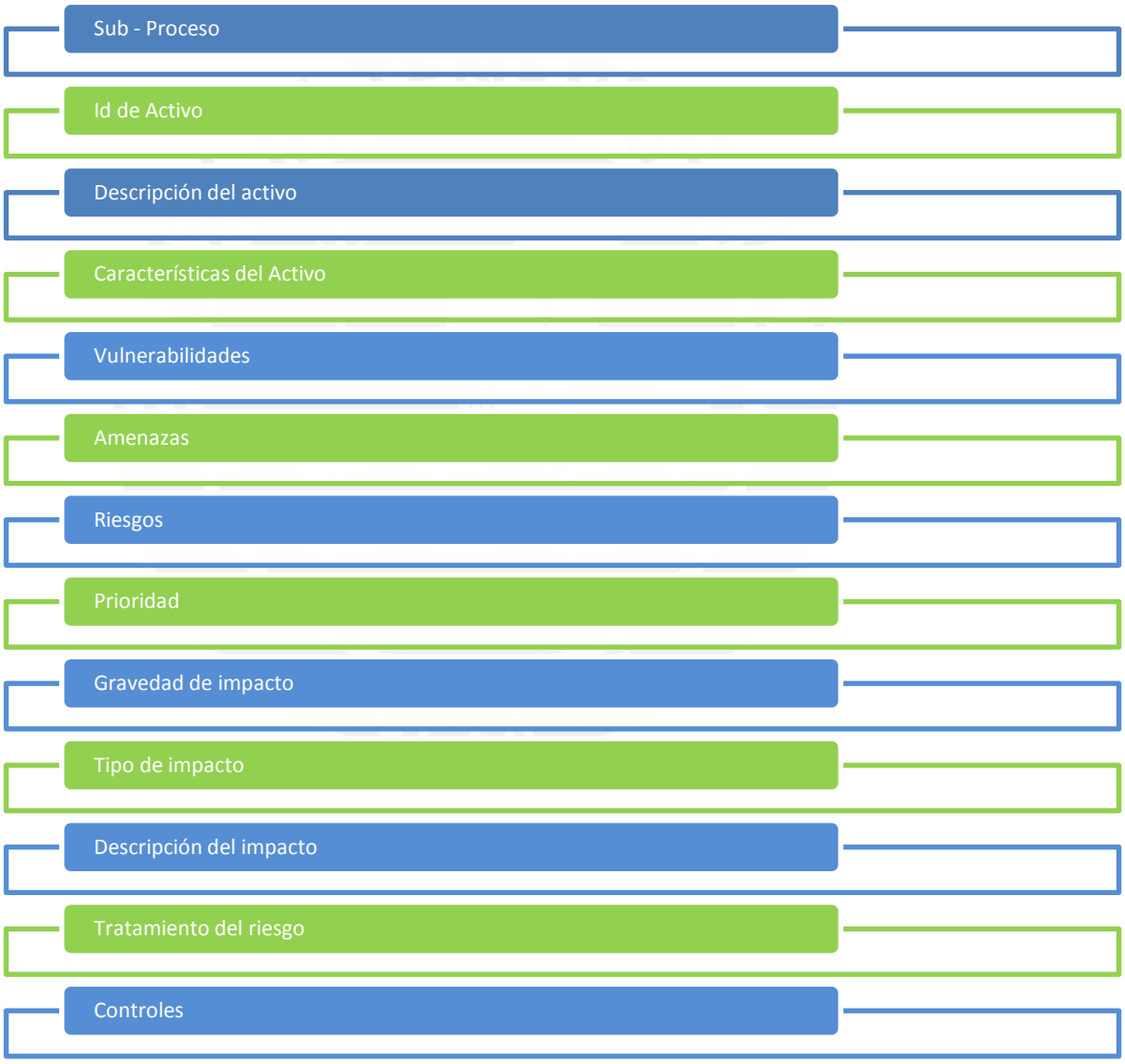
TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

empresas y así, clasificarlos por su criticidad. También facilita implantar los controles necesarios para tratar dichos riesgos asociados a los activos. [5]

Como se mencionó, para el análisis y gestión de riesgos de este proyecto se baso en la norma MAGERIT II, la cual cuenta con 4 etapas. Los resultados obtenidos en cada una de las etapas de plasmaron en diferentes, las cuales se muestran en los anexos de este documento.

En las distintas tablas se manejan las siguientes columnas:



A continuación se muestra como de desarrollo las etapas 2, 3 y 4 de la metodología MAGERIT para el análisis de riesgos en este proyecto de fin de carrera:

Tesis publicada con autorización del autor
No olvide citar esta tesis

3.1.1 Etapa 2: Análisis de Riesgos

Como *primera actividad* de esta etapa, se procedió a levantar la información necesaria para poder realizar el análisis. Luego de ese levantamiento de información y su análisis se decidió enfocarnos en el proceso de *producción* y sus 4 subprocesos (*planificación, manufactura, calidad, bodegas*) para poder realizar el análisis de riesgos ya que se considero que es el proceso más importante para la continuidad del negocio.

Como *segunda actividad* se procedió a identificar los activos involucrados en cada subproceso y sus características. Para cada activo identificado se asigno un código o Id. comprendido de 3 letras, dependiendo del tipo de activo que era, más un numero correlacionado, así los tipos de códigos usados fueron:

SIS	•Activo del tipo sistema de información o interfaz.
DOC	•Activo del tipo documento fisico o digital con información importante.
SW	•Activo del tipo software con información importante.
HW	•Activo del tipo hardware que maneja información importante.
AF	•Activo del tipo fisico ubicado dentro de la empresa.

Para mostrar esta información se realizaron unas tablas, las cuales se presentan en el ANEXO 1 de este documento. En estas tablas se presentan 5 columnas, las cuales se describen a continuación:

Subproceso (*Columna 1*)
•En esta columna se muestra cada uno de los subprocesos del proceso de producción, a los que le vamos a realizar el análisis de riesgos de sus activos.
Id. de Activo (*Columna 2*)
•En esta columna se le asigna un código de identificación a cada activo encontrado, el cual no servirá mas adelante para referenciar al activo en las demás tablas.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

Descripción del Activo (*Columna 3*)

- En esta columna se muestra el nombre de cada activo encontrado.

Características (*Columna 4*)

- En esta columna se listan las principales características de cada uno de los activos.

Como ***tercera actividad*** dentro de esta etapa se procedió a analizar e identificar las vulnerabilidades intrínsecas de los activos descritos anteriormente y las amenazas respectivas que podrían explotar estas vulnerabilidades y causar daño o afectar la continuidad del negocio.

La *vulnerabilidad* de un activo es la potencialidad o posibilidad de que se materialice una amenaza sobre dicho activo, forma parte del estado de seguridad del activo. Las *amenazas* son los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Para mostrar esta información se realizaron otras tablas, las cuales se presentan en el ANEXO 2 de este documento. En estas tablas se presentan 5 columnas, las cuales se describen a continuación:

Subproceso (*Columna 1*)

- En esta columna se muestra cada uno de los subprocesos del proceso de producción, a los que le vamos a realizar el análisis de riesgos de sus activos.

Id. de Activo (*Columna 2*)

- En esta columna se le asigna un código de identificación a cada activo encontrado, el cual no servirá más adelante para referenciar al activo en las demás tablas.

Activo (*Columna 3*)

- En esta columna se agrupan los activos pertenecientes a este subproceso, los cuales tiene la vulnerabilidad y amenaza mostradas en las columnas 4 y 5.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

Vulnerabilidad (*Columna 4*)

- En esta columna se muestran las diversas vulnerabilidades que puede tener cada activo o grupo de activos.

Amenaza (*Columna 5*)

- En esta columna se menciona la amenaza que puede explotar cada vulnerabilidad mencionada en la columna anterior.

En estas tablas del ANEXO 2, se presenta una tabla por cada subproceso que se está analizando, en la 2da columna agrupamos algunos activos, los cuales tiene la vulnerabilidad y amenaza presentados en las columnas 4 y 5. Por ejemplo, en la primera tabla de este anexo tenemos:

- En la primera columna se muestra el subproceso al que estamos haciendo mención con esta tabla que es el proceso de planificación.
- En la segunda columna agrupamos los activos SIS-01, SIS-02, SIS-03,SIS-04, SIS-05, SIS-06.
- Estos activos tienen la vulnerabilidad presentada en la columna 4, que es: "*Controles de acceso al sistema inadecuados*".
- Y esta vulnerabilidad puede ser explotada por la amenaza presenta en la siguiente columna, que es: "*Filtraciones de información y accesos no autorizados el sistema".*
- Esto se repite para el siguiente grupo de activos, que son los mismos que antes (SIS-01, SIS-02, SIS-03,SIS-04, SIS-05, SIS-06), y estos tiene la vulnerabilidad de "*Puntos de acceso al sistema remotos a la red privada de la empresa",* la cual puede ser explotada por la amenaza *"Accesos de personas no autorizadas al sistema e intercepción de la red".*
- Y así es sucesivamente en el resto de esta tabla y para las tablas de los demás subprocesos.

Como cuarta actividad de esta etapa se procedió con la identificación y evaluación de los riesgos asociados a las amenazas identificadas en las tablas del ANEXO 2. Esta actividad consistió en identificar los riesgos para cada activo y su amenaza correspondiente.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

El riesgo es el potencial de que una amenaza (externa o interna) explote una vulnerabilidad de uno o varios activos ocasionando daño a la organización. Su naturaleza puede depender de aspectos operativos, financieros, regulatorios (legales) y administrativos. [5]

Luego de identificar los riesgos para cada activo, analizamos la prioridad que se le debía dar al análisis y tratamiento de cada riesgo, dependiendo de la importancia que tiene el activo para la continuidad del negocio.

Como quinta actividad se realizó el análisis del impacto que tendría para la organización la materialización de cada riesgo. El impacto en un activo es la consecuencia que tendría sobre éste la materialización de una amenaza, es decir es la diferencia en las estimaciones del estado de seguridad del activo antes y después de la materialización de la amenaza sobre éste. Esta identificación del impacto abarcó identificar 3 características del mismo: gravedad, tipo y descripción del impacto.

Los resultados obtenidos de la cuarta y quinta actividad se muestran mediante tablas en el ANEXO 3 de este documento. En este anexo, al igual que en los 2 anteriores, se muestra una tabla por cada subproceso, las cuales tendrán las siguientes columnas:

Subproceso (*Columna 1*)

- En esta columna se muestra cada uno de los subprocesos del proceso de producción, a los que le vamos a realizar el análisis de riesgos de sus activos.

Id. de Activo (*Columna 2*)

- En esta columna se le asigna un código de identificación a cada activo encontrado, el cual no servirá más adelante para referenciar al activo en las demás tablas.

Amenaza (*Columna 3)*

- En esta columna se muestran las amenazas a las que estan expuestos los activos, las cuales se identificaron en el Anexo 2.

Riesgo (Columna 4)

- En esta columna muestra se el riesgo al que esta expuesto cada activo dependiendo de la amenaza.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Prioridad (Columna 5)

- En esta columna se muestra la prioridad que se le debe dar al tratamiento de cada riesgo dependiendo de la importancía del activo.

Gravedad del Impacto (Columna 6)

- En esta columna se indica la gravedad que tendría el impacto para la organización si es que se llegara a meterializar el riesgo.

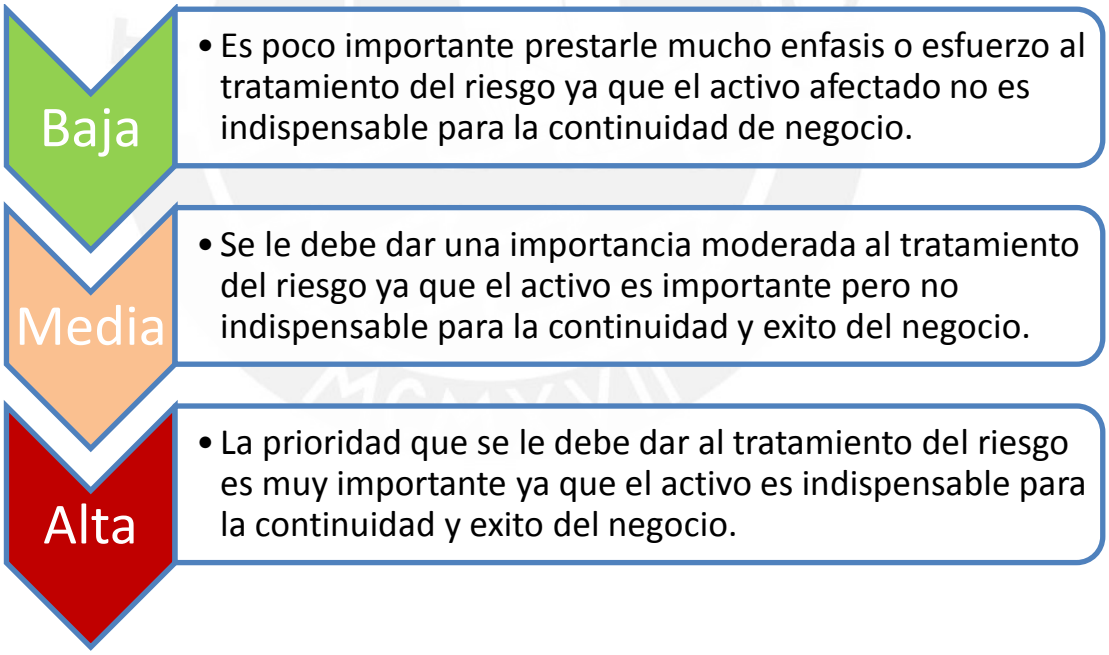
Tipo de Impacto (Columna 7)

- En esta columna se indica el tipo de impacto que generaría la materialización del riesgo.

Descripción del impacto (Columna 8)

- En esta columna se describe el impacto que generaría la materialización del riesgo

Para calificar la prioridad del riesgo se utilizó un rango de 3 valores, los cuales se describen a continuación:



Luego para analizar la gravedad del impacto se utilizo otro rango de valores, los cuales fueron asignados a cada impacto dependiendo del nivel de daño que causaría para la organización la materialización del riesgo en perjuicio del activo de información. Los valores para calificar la gravedad del impacto, fueron los siguientes:

Tesis publicada con autorización del autor
No olvide citar esta tesis

3.1.2 Etapa 3: Gestión de Riesgos

Como *primera actividad* de esta etapa, se procedió a realizar en análisis del tratamiento que se le debía dar a cada riesgo identificado. Una vez que conocemos los riesgos de la organización y decidido el tratamiento que se le va a dar a cada

Tesis publicada con autorización del autor
No olvide citar esta tesis

uno de los activos, se deben tomar acciones en consecuencia. Los 4 tipos de tratamiento requieren de acciones de distinta naturaleza:

Aceptar el Riesgo	• La dirección asume el riesgo ya que esta por debajo de un valor de riesgo aceptable, simplemente requiere que quede documentado que la dirección conoce y acepta estos riesgos. Los riesgos que se han asumido han de ser controlados y revisados periódicamente de cara a evitar que evolucionen y se conviertan en riesgos mayores.
Mitigar el Riesgo	• Reducirlo mediante la implantación de controles que reduzcan el riesgo a un nivel aceptable, implica seleccionar dichos controles, definir y documentar los métodos para ponerlos en marcha y gestionarlos.
Transferir el riesgo a un tercero	• Como por ejemplo, asegurando el activo que tiene el riesgo o subcontratando el servicio. Deben evaluarse las opciones y tomar las acciones pertinentes para ejecutar la opcón escogida, en funcion del valor del activo y del coste de realizar esta transferencia (no sólo coste económico sino tambien los riesgos que conlleva esta transferencia en cuanto a la inclusion de un tercero.
Eliminar el Riesgo	• Aunque no suele ser la opción más viable, ya que puee resultar difícil o demasiado costoso, si se cree posible o necesario, habrá que establecer los pasos para conseguirlo: eliminar el activo, eliminar el proceso o incluso el área de negocio que es la fuente del riesgo.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

Este análisis y selección de tratamientos escogidos para cada activo y riesgo identificado se muestra en el *ANEXO 4,* en el cual se muestran las siguientes columnas:

Id. de Activo (Columna 1)

- En esta columna se le asigna un código de identificación a cada activo encontrado.

Descripción del Activo (Columna 2)

- En esta columna se muestra el nombre de cada activo encontrado

Amenaza (Columna 3)

- En esta columna se muestran las amenazas a las que estan expuestos los activos, las cuales se identificaron en el Anexo 2.

Riesgo (Columna 4)

- En esta columna muestra se el riesgo al que esta expuesto cada activo dependiendo de la amenaza.

Tratamiento (Columna 5)

- En esta columna se muestra el tipo de tratamiento que se le debe dar a cada riesgo.

No caben más acciones a la hora de gestionar los riesgos para el correcto diseño de un sistema de gestión de seguridad de información, ya que una organización que conoce sus riesgos jamás podrá ignorarlos, puesto que, de este modo, no estaría vigilando que no se convirtiesen en riesgos que la organización no es capaz de asumir o que, por no haberlos tenido en cuenta, se materialicen y den lugar a incidentes de seguridad.

3.1.3 Etapa 4: Selección de Salvaguardas (Controles)

MAGERIT define la función o servicio de salvaguarda como acción genérica que puede reducir un riesgo, y el mecanismo de salvaguarda como el procedimiento o dispositivo, físico o lógico que lo reduce real y específicamente. Para reducir el riesgo, se necesita mejorar las salvaguardas existentes o incorporar otras nuevas.

La función o servicio de salvaguarda es una acción de tipo actuación (o no-actuación, es decir, omisión), fruto de una decisión para reducir un riesgo (no es una acción de tipo evento). Dicha actuación se materializa en el correspondiente mecanismo de salvaguarda que opera de 2 formas, en general alternativas:

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

- "Neutralizando" o "bloqueando" otra acción, que es el evento de materialización de la amenaza en forma de agresión, con una reducción previa al evento de la vulnerabilidad, mediadora de dicha materialización.
- Modificando de nuevo el estado de seguridad del activo agredido (modificado anteriormente por el impacto consecuente a la amenaza materializada), con una reducción posterior al evento productor de dicho impacto.

Las funciones o servicios y los mecanismos de salvaguarda se tipifican según su forma de actuación en 2 grandes tipos:

- Las funciones o servicios preventivos actúan sobre la vulnerabilidad (antes de la agresión) y reducen la potencialidad de materialización de la amenaza (no su posibilidad genérica, que es independiente del activo amenazado). Este tipo de función o servicio actúa sobre amenazas humanas, ya sean involuntarias o intencionales.
- Las funciones o servicios curativos o restablecedores actúan sobre el impacto tras la agresión) y reducen su gravedad. Este tipo de función o servicio puede actuar en general con amenazas de todos los tipos.

3.1.3.1 Salvaguardas preventivas

- *La concienciación, información y formación* del personal propio y del relacionado establemente con la organización es un tipo de salvaguarda "estructural" (ligada a la estructura global de la organización y no sólo a sus sistemas de información). Su importancia se justifica por el papel esencial que juega en la seguridad el factor humano.
- *La disuasión* es un tipo de salvaguarda que empuja a reconsiderar el inicio de la agresión por el potencial agresor humano intencional, a partir de las consecuencias que puedan sobrevenirle contra su propio interés. Este tipo de salvaguarda exige normalmente una difusión lo más amplia –y a la vez selectiva- posible. Por ejemplo, el establecimiento de condenas por el Código Penal es una de las salvaguardas de disuasión más conocidas.
- *La prevención* propiamente dicha es un tipo de salvaguarda de protección que no impide el inicio de la materialización de la amenaza, solo su realización completa y por lo tanto la materialización plena del impacto. Como ejemplo puede tomarse el control de accesos.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

- *La detección preventiva* puede llegar a ser disuasoria, si su existencia es conocida por el potencial agresor, y éste es consciente de que podría ser descubierto.

3.1.3.2 Salvaguardas curativas y restablecedoras

- La corrección es un tipo de salvaguarda que impide la propagación del impacto resultante de la amenaza materializada y limita así los efectos de ésta. Por ejemplo, un impacto en la integridad de una información que se detecte por un descuadre lleva a tomar medidas limitadoras que paralizan la circulación de dicha información y verifican fuentes.
- La recuperación es un tipo de salvaguarda restauradora que repara o reconstruye los elementos dañados para acercarse al estado de seguridad previo a la agresión del activo agredido. Si no basta la recuperación funcional, pueden adoptarse también otras salvaguardas como la transferencia del riesgo a terceros (por ejemplo con los seguros) o la acción ante los tribunales.
- La detección curativa, “monitorización” o seguimiento curativo del impacto, en caso de amenaza materializada, es previa a toda eficacia en la actuación de las salvaguardas curativas (muchas agresiones son detectadas tarde o no son detectadas nunca). El cuadre de la información sería un buen ejemplo de esta salvaguarda detectora.

Para el análisis y selección de salvaguardas (controles) adecuados para tratar cada riesgo identificado en la etapa anterior, se utilizo la norma ISO/IEC 270002. Esta norma considera que los controles esenciales para una organización desde un punto de vista legislativo comprenden:

- La protección de los datos de carácter personal y la intimidad de las personas.
- La salvaguarda de los registros de la organización.
- Los derechos de la propiedad intelectual.

Los controles que se consideran la mejor práctica habitual para conseguir la seguridad de la información comprenden:

- La documentación de la política de seguridad de la información.
- La asignación de responsabilidades de seguridad.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

- La formación y capacitación para la seguridad de la información.
- El procedimiento correcto en las aplicaciones.
- La gestión de la vulnerabilidad técnica.
- La gestión de la continuidad del negocio.
- El registro de las incidencias de seguridad y las mejoras.

Según esta norma, estos controles pueden aplicarse a la mayoría de las organizaciones y los entornos.

Este estándar contiene 11 clausulas de control de seguridad que contienen colectivamente un total de 39 categorías principales de seguridad y una clausula introductoria conteniendo temas de evaluación y tratamiento del riesgo. Las 11 clausulas son:

a. Política de seguridad. (PS)
b. Organizando la seguridad de información. (OS)
c. Gestión de activos. (GA)
d. Seguridad en recursos humanos. (SRH)
e. Seguridad física y ambiental. (SFA)
f. Gestión de comunicaciones y operaciones. (GC)
g. Control de acceso. (CA)
h. Adquisición, desarrollo y mantenimiento de sistemas de información. (ADM)
i. Gestión de incidentes de los sistemas de información. (GI)
j. Gestión de la continuidad del negocio. (GCN)
k. Cumplimiento. (CM)

En el ANEXO 5 de este documento se presenta en una tabla los controles planteados para tratar cada riesgo identificado en los activos de la empresa. En esta tabla se muestran las siguientes columnas.

Id de activo (Columna 1) (Id)

- En esta columna se le asigna un código de identificación a cada activo encontrado. Para el caso de los sistemas y documentos de cada subproceso, se agruparon estos tipos de activos ya que los controles se repiten.

Riesgo (Columna 2) (RN)

- En esta columna muestra se el riesgo al que esta expuesto cada activo dependiendo de la amenaza. La letra N de las silgas RN indica el numero de riesgo del activo, por ejemplo: R1 es el riesgo numero 1 y R2 es el riesgo número 2.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Clausula de la norma ISO 27002 (Columna 4) (Clau)

- En esta columna se muestra cual de las 11 clausulas de la norma, se aplica para este riesgo. Para mostrar las clausulas se usa las abreviaturas que se encuentran entre parentesis al lado de cada una, en el listado anterior, por ejemplo: Politica de Seguridad = PS, Control de Acceso (CA).

Control 1 (Columna 5)

- En esta columna de muestra el primer control planteado.

Control 2 (Columna 6)

- En esta columna de muestra el segundo control planteado.

Control 3 (Columna 7)

- En esta columna de muestra el tercer control planteado.

Control 4 (Columna 8)

- En esta columna de muestra el cuarto control planteado.

Luego de terminado el planteamiento de los controles adecuados para tratar los riesgos identificados, se continuo con desarrollar los planes o guías de implementación de estos controles.

Un plan o guía de implementación de controles de seguridad, sirve como ayuda para que la empresa pueda realizar estas implementaciones de manera adecuada, ordenada y gradual.

Para no hacer un plan o guía de implementación de cada uno de los controles planteados en el Anexo 5, ya que son una gran cantidad, se decidió desarrollar un plan de implementación para cada clausula de control de seguridad que se planteo, a las cuales pertenecen los controles. Como se mostro en la tabla del Anexo 5, las clausulas planteadas fueron:

- Política de seguridad. (PS)
- Seguridad física y ambiental. (SFA)
- Gestión de comunicaciones y operaciones. (GC)
- Control de acceso. (CA)

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

- Adquisición, desarrollo y mantenimiento de sistemas de información. (ADM)

Para desarrollar estas guías de implementación, se baso en las guías de implementación que se recomiendan en la norma ISO/IEC 27002. El desarrollo y documentación de estas guías de implementación se muestra en el *Anexo 6* de este documento de tesis.

3.2 Políticas de Seguridad

Luego de haber terminado con el análisis y gestión de riesgos, para completar el diseño del SGSI planteamos algunas políticas de seguridad para garantizar el buen funcionamiento del SGSI.

Las políticas de seguridad son los estándares coherentes de seguridad a nivel de gerencia, usuarios y personal técnico que salvaguardan los activos de información manteniendo un balance adecuado entre el proceso de controlar (costo y esfuerzo para establecer y monitorear controles) y la productividad (los controles no deben complicar la labor de los usuarios de TI). Son documentos de alto nivel que revelan la filosofía corporativa y el pensamiento estratégico de la organización. Las políticas además deben ser aprobadas por Alta Gerencia; debe ser documentada y distribuida a los involucrados: usuarios internos y externos (proveedores) para definir las responsabilidades de cada uno de ellos. Las políticas de seguridad deben ser revisadas y actualizadas periódicamente a intervalos planificados o si ocurriesen cambios en la infraestructura de SI – TI.

En este proyecto de tesis se han documentado las siguientes políticas de seguridad:

- Política de asignación de equipos.
- Política de desarrollo de aplicaciones.
- Política de cambios a sistemas de aplicación.
- Política de protección de la información y escritorio limpio.
- Política de usuarios privilegiados.
- Política de retención de documentos.

La documentación de cada una de estas políticas, se presenta en el Anexo 7 de este documento de tesis.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

CAPÍTULO 4 CONCLUSIONES, RECOMENDACIONES Y TRABAJOS FUTUROS

En el presente capítulo se presentarán las conclusiones, recomendaciones y trabajos futuros correspondientes al diseño de un SGSI para una empresa de producción de alimentos de consumo masivo.

4.1 CONCLUSIONES

Tal como se describió y presento a lo largo de este proyecto de fin de carrera, la adecuada gestión de la seguridad de información es algo que debe estar ya incluido en la cultura organizacional de las empresas; y en todas ellas esta adecuada gestión no se lograría sin el apoyo de la alta gerencia como promotor activo de la seguridad en la empresa.

Debe tenerse en cuenta que el diseño de SGSI presentado se adapta a los objetivos actuales del proceso de producción, en el cual se ha basado el proyecto, y que este diseño podría variar ya que los objetivos estratégicos y de gobierno de le empresa pueden cambiar y por ello algunos sub procesos que forman parte del alcance del proyecto, también lo harán.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

Del mismo modo, se debe establecer que los dueños de cada uno de los procesos que fueron analizados para el diseño del SGSI de este proyecto, empiecen a darle mayor importancia a la seguridad de la información, y que velen para que de alguna manera se pueda levantar los riesgos encontrados dentro de sus actividades ya que no es seguro que este diseño se logre implementar, y por ello debería ser labor de ellos el tratar de eliminar dichos riesgos.

4.2 RECOMENDACIONES Y TRABAJOS FUTUROS

En primera instancia se recomienda a la empresa de producción de alimentos de consumo masivo que en base al diseño presentado en este proyecto, se dedique en concientizar a todos los empleados que forman parte de dicha empresa, sobre la seguridad de la información y su importancia, y realizar evaluaciones periódicas a los indicadores de seguridad de la empresa y de los riesgos encontrados.

Luego, se recomienda aplicar esfuerzos para poder realizar la implementación de este diseño para que permita que en el futuro se pueda gestionar la seguridad de información de tal manera que se pueda aspirar a una certificación, ya que el diseño ha sido realizado con la norma ISO/IEC 27001, la cual es certificable.

Como trabajos futuros se pueden realizar diseños similares para los demás procesos de la empresa. De manera similar sería adecuado que se elabore un plan de continuidad de negocio, lo que permitirá reforzar la seguridad en la empresa y además de diseñar un plan de auditoría que se realice periódicamente para analizar cómo va variando el nivel de seguridad de la empresa tal como avanza el tiempo.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

REFERENCIAS

[1] Ampuero Chang, Carlos

2011 Diseño de un Sistema de Gestión de Seguridad de Información para una compañía de Seguros. Tesis para optar por el título de Ingeniero Informático. Lima: Pontificia Universidad Católica del Perú, Facultada de Ingeniería Informática. http://tesis.pucp.edu.pe/repositorio/handle/123456789/362.

[2] ALEXANDER G., Alberto

2007 Diseño de un Sistema de Gestión de Seguridad de Información / Óptica ISO/ IEC 27001:2005. Primera edición. Bogotá: Alfaomega Colombiana S.A.

[3] Fernández, Eduardo y Mario Piattini

2003 Seguridad de las tecnologías de la Información: La construcción de la confianza para una sociedad conectada. Primera edición. Madrid: Ediciones Aenor.

[4] García, Alfonso y María del Pilar Alegre

2011 Seguridad Informática. Primera edición. Madrid: Ediciones Paraninfo SA.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

[5] Tupia, Manuel

2011 Principios de auditoría y control de sistemas de información. Segunda edición. Lima: Tupia Consultores y Auditores.

[6] Villena, Moises

2006 Sistema de Gestión de Seguridad de Información para una compañía de Seguros. Tesis para optar por el título de Ingeniero Informático. Lima: Pontificia Universidad Católica del Perú, Facultada de Ingeniería Informática.
http://tesis.pucp.edu.pe/repositorio/handle/123456789/933

[7] Donado, Siler Amador y Flechas Andrés

2001 Seguridad Computacional. Primera edición Cauca.
http://www.govannom.org/seguridad/seg_general/seg_com.pdf

[8] Qualitas Consultores

2012 Normas: ISO/ IEC 27001
http://qualitas.com.pe/normas/iso-27001

[9] INTERNATIONAL STANDARD ISO/IEC 27003

2010 Information technology — Security techniques — Information security management system implementation guidance. Primera Edición

[10] ISSA

2011 ISO/ IEC 27004. Lima
http://issaperu.org/?p=13

[11] Instituto nacional de Tecnologías de comunicación

2011 Enciclopedia Jurídica: ISO/IEC 27005:2008.
http://www.inteco.es/wikiAction/Seguridad/Observatorio/area_juridica_seguridad/Enciclopedia/Articulos_1/iso_27005_en

[12] INTERNATIONAL STANDARD ISO/IEC 27006

2007 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

management systems. First Edition.
http://www.pqm-online.com/assets/files/standards/iso_iec_27006-2007.pdf

[13] INTERNATIONAL STANDARD ISO/IEC 27007
2011 Information technology — Security techniques — Guidelines for information security management systems auditing. First Edition.

[14] Hernandez, Alejandro
2008 Seguridad de la Información: Norma ISO/ IEC 17799 / ISO/ IEC 27001. Consulta: 13/04/2012.
http://www.slideshare.net/disalazar/certificacion-iso-27001-isecsegurity-presentation

[15] ISO27000.es
2005 ISO 27001: Auditoria y Certificación. Consulta: 14/04/2012.
http://www.iso27000.es/certificacion.html#section5b

[16] ISMS International User Group
2012 ISMS Certificates. Consulta: 13/04/2012.
http://www.iso27001certificates.com/

[17] INTERNATIONAL STANDARD ISO/IEC 27001
2005 Information technology — Security techniques — Information security management system— Requirements. Primera Edición.

[18] INTERNATIONAL STANDARD ISO/IEC 27002
2005 Information technology — Security techniques — Code of practice for information security management. Primera Edición.

[19] CNN EXPANSIÓN
2012 El verdadero costo del cibercrimen. Consulta: 14/06/2012.
http://www.cnnexpansion.com/tecnologia/2011/08/12/delito

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

[20] Informatica Jurídica

2012 La formación de empleados como elemento fundamental para proteger la información de nuestra empresa. Consulta: 14/06/2012. http://www.informatica-juridica.com

[21] SELDON, Arthur

1975 Diccionario de Economía. Tomo único. 2da Edición. Barcelona: Industrias Gráficas García.

Tesis publicada con autorización del autor
No olvide citar esta tesis