ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSTGRADOS

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN GERENCIA DE SISTEMAS

TEMA: DISEÑO PARA LA IMPLEMENTACIÓN DE LOS DOMINIOS DE CIFRADO Y SEGURIDAD FÍSICA Y AMBIENTAL BASADOS EN LA NORMA ISO27001 E ISO27002, PARA EL ÁREA DE TI DE LA PROCESADORA NACIONAL DE ALIMENTOS "PRONACA"

AUTORES:

ING. RAMÍREZ JARAMILLO CARLOS DANIEL

ING. MOREIRA ZAMBRANO ROLANDO MAURICIO

DIRECTOR:

ING. CAMPAÑA ORTEGA MAURICIO M.I.S, M.D.U.

SANGOLQUÍ – ECUADOR

2017

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE VICERECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

CERTIFICADO

Que el trabajo titulado DISEÑO PARA LA IMPLEMENTACIÓN DE LOS DOMINIOS DE CIFRADO Y SEGURIDAD FÍSICA Y AMBIENTAL BASADOS EN LA NORMA ISO27001 E ISO27002, PARA EL ÁREA DE TI DE LA PROCESADORA NACIONAL DE ALIMENTOS "PRONACA", ha sido realizado por los Ingenieros: Carlos Daniel Ramírez Jaramillo y Rolando Mauricio Moreira Zambrano.

De la misma manera ha sido tutelado periódicamente y revisado en su totalidad, cumpliendo con las normas establecidas por la ESPE, en el reglamento de estudiantes de la Universidad de las fuerzas Armadas.

El mencionado trabajo consta de un disco compacto, el que contiene todos los archivos en formato digital.

Para los fines pertinentes, se autoriza a los Ingenieros Carlos Daniel Ramírez Jaramillo y Rolando Mauricio Moreira Zambrano que lo entregue a la Biblioteca Alejandro Segovia.

Sangolquí, junio 2017

Ing. Mauricio Campaña Ortega M.I.S, M.D.U.

ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE POSTGRADOS

MAESTRÍA EN GERENCIA DE SISTEMAS

AUTORÍA DE RESPONSABILIDAD

Yo, **CARLOS DANIEL RAMÍREZ JARAMILLO**, con cédula de identidad N° 1710043082 Yo, **ROLANDO MAURICIO MOREIRA ZAMBRANO**, con cédula de identidad N° 1310889033, declaramos que este trabajo de titulación **DISEÑO PARA LA IMPLEMENTACIÓN DE LOS DOMINIOS DE CIFRADO Y SEGURIDAD FÍSICA Y AMBIENTAL BASADOS EN LA NORMA ISO27001 E ISO27002, PARA EL ÁREA DE TI DE LA PROCESADORA NACIONAL DE ALIMENTOS "PRONACA"** ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaramos que este trabajo es de nuestra autoría, en virtud de ello nos declaramos responsables del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 15 de junio de 2017

Ing. Carlos Daniel Ramírez J.
C.C. 1710043082

Ing. Rolando Mauricio Moreira Z.
C.C. 1310889033

ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE POSTGRADOS

MAESTRÍA EN GERENCIA DE SISTEMAS

AUTORIZACIÓN

Yo, **CARLOS DANIEL RAMÍREZ JARAMILLO**, Yo, **ROLANDO MAURICIO MOREIRA ZAMBRANO**, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación **DISEÑO PARA LA IMPLEMENTACIÓN DE LOS DOMINIOS DE CIFRADO Y SEGURIDAD FÍSICA Y AMBIENTAL BASADOS EN LA NORMA ISO27001 E ISO27002, PARA EL ÁREA DE TI DE LA PROCESADORA NACIONAL DE ALIMENTOS "PRONACA"** cuyo contenido, ideas y criterios son de nuestra autoria y responsabilidad.

Sangolquí, 15 de junio de 2017

Ing. Carlos Daniel Ramirez J.
C.C. 1710043082

Ing. Rolando Mauricio Moreira Z.
C.C. 1310889033

DEDICATORIA

La presente tesis se la dedico a DIOS con todo mi corazón debido a que la Gloria y Honra le pertenecen única y exclusivamente a Él.

A Kendra

Tenerte a ti fue mi elección, he renunciado a muchas cosas en la vida y antes de pensar en mí, siempre pensé en ti porque fuiste parte importante de ella.

Gracias por brindarnos tu cariño y lealtad demostrada durante toda tu existencia, ahora que no te encuentras dejas una hermosa trascendencia en cada uno de nosotros.

A mi madre Sra. MARIANITA JARAMILLO A.

Por ser uno de los pilaras más importantes en mi vida, demostrándome su amor incondicional desde mi infancia, ejemplos dignos de superación y entrega, lo cual me ha servido para salir adelante en los momentos más difíciles.

A mi padre Magister CARLOS RAMÍREZ S.

Por su cariño y esfuerzo demostrado incondicionalmente, quien siempre ha estado en la totalidad de mi formación tanto académica como espiritual, alentándome para culminar con éxitos las objetivos trazados donde los principios y valores inculcados jamás han sido negociables.

A mi hermanita Ing. JOHANNA RAMÍREZ J.

Por su total comprensión, ternura e infinita paciencia al haber cuidado completamente de Kendrita, su fiel compañera.

Ing. Carlos Daniel Ramírez J.

DEDICATORIA

El presente trabajo se lo dedico a mis padres Mauricio Gualberto Moreira García y Nittza María Zambrano Alcívar, mi apoyo de toda la vida.

Ing. Rolando Moreira Z.

AGRADECIMIENTOS

A la noble y gloriosa institución UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE, porque en sus aulas recibí el conocimiento intelectual lleno de principios y ética para servir al prójimo.

A mi Director de tesis, Magister MAURICIO CAMPAÑA ORTEGA, por su inestimable ayuda y paciencia quien ha sabido transmitir su conocimiento para el desarrollo de éste proyecto.

Al Coordinador del Programa de Maestría en Gerencia de Sistemas, Magister GEOVANNI NINAHUALPA QUIÑA, por la acertada orientación proporcionada en el trabajo realizado.

Al Magister CARLOS PRÓCEL SILVA, porque en ésta ocasión no ha sido la excepción de su gestión realizada y le agradezco por ayudarme a lograr esta nueva meta, mi maestría.

CARLOS DANIEL RAMÍREZ JARAMILLO

AGRADECIMIENTOS

Agradezco en primer lugar a Dios ya que sin él nada es posible.

A mis padres, MAURICIO GUALBERTO MOREIRA GARCÍA y NITTZA MARÍA ZAMBRANO ALCIVAR que gracias a su apoyo incondicional en todo momento pude conseguir la motivación para seguir adelante.

Al Ingeniero, MAURICIO CAMPAÑA e Ingeniero GEOVANNI NINAHUALPA, quienes con su apoyo supieron guiarme y darme las pautas para la culminación de este trabajo.

Finalmente, a mis compañeros y amigos que creyeron en mi durante todo este trayecto en los altos y bajos hasta llegar a la ansiada meta.

ROLANDO MAURICIO MOREIRA ZAMBRANO

ÍNDICE

CAPÍTULO I 1
INTRODUCCIÓN 1
1.1 Generalidades 1
1.2 Antecedentes 2
1.3 Planteamiento del problema. 2
1.4 Justificación e importancia. 3
1.5 Objetivos 4
1.5.1 Objetivo General 4
1.5.2 Objetivos específicos 4
1.6 Alcance. 5
CAPÍTULO II 6
MARCO TEÓRICO 6
2.1 Introducción 6
2.2 Definición de seguridad de la información 6
2.3 Riesgos 7
2.3.1 Concepto de Riesgo 8
2.3.2 Evaluar los riesgos de la seguridad de la información 8
2.3.3 Análisis del riesgo 8
2.3.4 Proceso de gestión del riesgo 8
2.3.5 En un SGSI se han establecido los siguientes procesos: 9
2.3.6 Principios de gestión del riesgo. 10
2.3.7 Clasificación de los activos. 11
2.3.8 Criterios Básicos de la gestión del riesgo 12
2.3.9 El alcance y límites del riesgo 15
2.3.10 Identificación del riesgo 16
2.3.11 Identificación de las vulnerabilidades 16
2.3.12 Reducción del Riesgo 18
2.3.13 Monitoreo y revisión de los factores de riesgo 19
2.4 Normas ISO 27000 21
2.4.1 Origen 22

2.4.2 Definición de las normas ISO 27000 23
2.4.3 Estándar ISO/IEC 27001 27
2.4.4 Estándar ISO/IEC 27002 42
CAPÍTULO III 43
SITUACIÓN ACTUAL DE PRONACA 43
3.1 Antecedentes históricos y legales de la organización 43
3.2 Historia. 44
3.3 Localización 47
3.4 Zona de Influencia 48
3.5 Misión y Visión 49
3.6 Organigrama de TI 54
3.7 Cadena de Valor de PRONACA. 54
3.8 Análisis de la situación actual de la seguridad informática en Pronaca 55
3.8.1 Permisos o privilegios de usuarios. 55
3.8.2 Password o contraseñas 55
3.8.3 Inactividad de equipos. 56
3.8.4 Uso de internet 56
3.8.5 Acceso al Data Center 57
3.8.6 Administración y control de acceso a la Información 58
3.8.7 Adquisición de bienes y servicios de Tecnología. 59
3.8.8 Adquisición de nuevos proyectos de tecnología. 60
3.8.9 Evaluación y riesgo tecnológico 61
3.8.10 Seguridad de incidentes del personal. 62
CAPÍTULO IV 65
IMPLEMENTACIÓN DE DOS DOMINIOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA PRONACA. 65
4.1 Cifrado 67
4.1.1 Controles Criptográficos 67
4.2 Seguridad física y ambiental 68
4.2.1 Áreas Seguras 68
4.2.2 Equipo de seguridad 70

CAPITULO V..... 74
CONCLUSIONES Y RECOMENDACIONES. 74
5.1 Conclusiones. **74**
5.2 Recomendaciones. **75**
REFERENCIAS BIBLIOGRÁFICAS Y ELECTRÓNICAS 77

ÍNDICE DE FIGURAS

Figura 1: Proceso de gestión del riesgo (UNE-ISO 31000) 9
Figura 2: Proceso de gestión del riesgo (Deming 1989) 10
Figura 3: Principios de gestión del riesgo (SGS, 2013) 11
Figura 4: Clasificación de Activos (SGS, 2013). 12
Figura 5: Ejemplo de Área de Impacto (MENDOZA, 2014) 13
Figura 6: Reducción del Riesgo 18
Figura 7: Historia de ISO 27001. (ISO2700.ES, 2012). 22
Figura 8: Evolución ISO 27000. (ISO27000.es, 2005). 23
Figura 9: Encuesta ISO sobre certificaciones de la norma para sistemas de gestión. (Rhand Leal, 2012) 28
Figura 10: Ciclo de adaptación de la Norma (SGS, 2013). 29
Figura 11: Dominios ISO27001 (SGS, 2013). 30
Figura 12: Cláusulas Objetivos y Controles de la Norma ISO 27002..... 42
Figura 13: INDIA en sus inicios 44
Figura 14: Inicio-Creación de la Compañía 45
Figura 15: Planta de conservas COMANA, INAEXPO 46
Figura 16: PRONACA Matriz: Av. De Los Naranjos 4415 y Av. Granados 47
Figura 17: PRONACA en el Ecuador 48
Figura 18: PRONACA en el Mundo 48
Figura 19: Productos de PRONACA 50
Figura 20: Estructura Organizacional 53
Figura 21: Dirección de TI 54
Figura 22: Cadena de Valor 54
Figura 23: Mapa conceptual de los 2 dominios de la norma ISO 27002. (ISO2700.ES, 2012) 66

RESUMEN

El objetivo del presente proyecto, se ha enfocado en el desarrollo de un Sistema de Gestión de Seguridad de la Información, establecida en los dominios de Cifrado y Seguridad Física y Ambiental de las normas ISO 27001 e ISO 27002 para el área de Software de la Procesadora Nacional de Alimentos PRONACA. Los dominios se expusieron basados en una investigación de las políticas y normas existentes en PRONACA. El dominio de Cifrado permitirá el resguardo de la información en base al análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.
Seguridad Física y Ambiental, minimizara las alarmas de daños e interferencias a la información y a las operaciones de la organización.

PALABRAS CLAVE:
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.
ISO.
PROCESADORA NACIONAL DE ALIMENTOS.
POLÍTICAS.
NORMAS.

ABSTRACT

The objective of this project has focused on developing a management system for information security, based domains Encryption, Physical Security, Environmental and Business Continuity ISO 27001 and ISO 27002 standards for the area Software of the National Food Processing PRONACA. The domains were proposed based on an analysis of existing policies and standards in PRONACA. The domain Encryption will protect information based on risk analysis performed, in order to ensure adequate protection of their confidentiality and integrity. Physical and Environmental minimize the risk of damage and interference to information and operations security organization.

KEY WORDS:
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.
ISO.
PROCESADORA NACIONAL DE ALIMENTOS.
POLÍTICAS.
NORMAS.

CAPÍTULO I
INTRODUCCIÓN

1.1 Generalidades

Cada vez que el tema de seguridad se convierte en un punto muy crítico y al mismo tiempo crucial para todas las empresas a nivel internacional. En la actualidad, con la dispersión del internet y con el uso de más mecanismos electrónicos en el ámbito empresarial el riesgo se ha intensificado considerablemente.

En el año 2015 el sector corporativo fue objeto de numerosos acontecimientos de seguridad en el que divulgaciones de vulnerabilidades afectaron a millones de dispositivos móviles, además que existieron noticias de ataques dirigidos, y en el que surgieron vulnerabilidades que afectaron a muchos mecanismos y en 2016 el número de casos aumentó afectando a más plataformas y tecnologías.

Con el desarrollo del presente proyecto, se obtendrá un sistema de gestión de los dominios de cifrado y seguridad física y ambiental basados en la norma ISO27001 e ISO27002, para el área de software de la procesadora nacional de alimentos “PRONACA”.

Los dominios se plantearon basados en un análisis de las políticas y normas existentes en PRONACA. El dominio de Cifrado permitirá la protección de la información en base al análisis de riesgo efectuado, con el fin de cerciorar una adecuada protección de su confidencialidad e integridad.

La Seguridad Física y Ambiental para minimizará los riesgos de daños e interferencias a la información y a las operaciones de la organización.

Las normas ISO27001 e ISO27002, dependiendo de la organización, recomienda controles para tener un óptimo manejo de su información, aplicaciones, seguridades, etc.

1.2 Antecedentes

La Procesadora Nacional de Alimentos “PRONACA”, es el resultado de años de trabajo, creatividad y constancia. Como empresa procesadora y comercializadora de alimentos ha alcanzado el reconocimiento por la alta calidad de sus productos que provienen de los sectores: cárnico, acuacultura y agroindustrial.

Es una empresa altamente comprometida con el perfeccionamiento de la calidad de vida de sus consumidores, clientes y colaboradores. Trabaja esmeradamente en la preparación de productos cien por ciento confiables, ofrece muchas fuentes de empleos y finalmente apoya al desarrollo de las zonas rurales del país.

Por el gran volumen y extensión de la compañía, es de suma relevancia que la información se encuentre protegida, aún más que se encuentre disponible en todo momento, para lo cual se debe implantar políticas y controles de Seguridad Informática, que sean capaces de evitar o al menos mitigar al máximo las amenazas constantes que puedan afectar a los sistemas e información.

1.3 Planteamiento del problema.

PRONACA, al ser una compañía diligente a la producción de alimentos para consumo humano y balanceado para animales, se encuentra estratégicamente posicionada a nivel nacional con diversas oficinas y una matriz situada en la ciudad de Quito-Ecuador, así mismo cuenta con muchos centros de distribución y plantas productoras, siendo sumamente importante la comunicación entre los usuarios de cada centro a través de aplicaciones y sistemas que posee la

compañía, creando de cierta manera vulnerabilidad de los accesos a la información, poniendo en riesgo este activo sumamente importante, debido a que no cuenta con políticas de seguridad claramente definidas o preventivas que permitan resguardar y proteger la información, además ya que el volumen de transaccionalidad diario es muy alto, provoca de esta manera que las bases de datos se llenen dejando inactivos los sistemas varios minutos, desencadenando en un malestar al usuario y retrasos en el despacho de la producción.

1.4 Justificación e importancia.

Cada día más y más individuos mal intencionadas intentan ingresar y robar información de la empresas. El acceso no autorizado a una red informática o equipos de la empresa puede ocasionar graves problemas. Por lo tanto, es fundamental saber qué recursos de la compañía necesitan protección y así controlar el acceso al sistema y los niveles de privilegios de todos los usuarios en el sistema de información. El objetivo de la seguridad informática es mantener la Integridad, Disponibilidad, Privacidad, Control y Autenticidad de la información manejada por computadora.

El desarrollo de este diseño, tiene como plan realizar e implementar un Sistema de Gestión de Seguridad de la Información (SGSI), para la Procesadora Nacional de Alimentos “PRONACA” en el área de Software, de manera que el objetivo principal sea obtener confiabilidad y disponibilidad al momento de interactuar con los Sistemas tanto internos como externos. La empresa carece en su totalidad con políticas internacionales de SGSI como lo es la ISO 27001.

La falta de visión al no constituir políticas de seguridad de la información, repercute considerablemente en varios componentes y se los podría minimizar considerablemente, como son el tiempo de respuesta ante eventualidades con

los sistemas y aplicaciones de la compañía, posibles ataques tanto internos como externos afectando la privacidad de la Información.

La información en PRONACA es un activo sumamente importante, ya que los sistemas y aplicaciones poseen fórmulas de los distintos productos que ofrece la compañía, estudios de mercadeo, estadísticas, informes contables y financieros, por esto es imprescindible contar con políticas claramente establecidas para evitar el acceso de personas malintencionadas a esta información, provocando perjuicios de un valor incalculable con magnas consecuencias financieras e intelectuales.

Es transcendental para PRONACA, el desarrollo e impulso del diseño de implementación de un SGSI, porque de esta manera se pondría continuar con las sistematizaciones de manera confiable y positiva.

1.5 Objetivos

1.5.1 Objetivo General

Implementar dominios de cifrado, seguridad física y ambiental mediante un SGSI basados en la norma ISO27001 e ISO27002, para el área de Tecnología de la Información (TI) de la Procesadora Nacional De Alimentos “PRONACA”.

1.5.2 Objetivos específicos

- Determinar la situación actual de seguridad de la Procesadora Nacional de Alimentos “PRONACA”.
- Analizar y Describir los dominios más importantes para la empresa en base a la situación actual de la empresa.
- Diseñar la propuesta de un SGSI en base a los estándares ISO 27001 e ISO 27002.

1.6 Alcance.

Se proyecta obtener un diseño de políticas de seguridad, con todos los lineamientos que demanda la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) según la Norma Internacional ISO 27002, en los dominios de cifrado, seguridad física y ambiental.

CAPÍTULO II
MARCO TEÓRICO

2.1 Introducción

Al igual que en el resto del mundo, las compañías en el Ecuador, consideran la información como un activo muy importante, indudablemente dándole prioridad y buscando opciones de control ante los accesos de manera cuidadosa, a más de buscar alternativas para tenerla disponible en cualquier momento.

Por esta razón se ha investigado maneras de obtener la mejor combinación entre la gestión de usuarios y la tecnología, encargados de establecer políticas de seguridad, tomando en cuenta estándares propuestos por entes regulatorios, que entregan herramientas y recomendaciones para un control eficaz y eficiente de la información, jugando un papel muy importante el cifrado, la seguridad física y ambiental.

2.2 Definición de seguridad de la información

El bien más apreciable de una empresa es la información, por lo que es de suma importancia protegerla y mantenerla fuera del alcance de personas malintencionadas que aspiren aprovechar dicha información.

Debido a que la información puede ser expuesta en diversas formas es demandante conservarla de una manera muy cuidadosa y segura, para que pueda ser utilizada en cualquier instante.

Cabe mencionar que la seguridad total de la información no existe, pero se puede mitigar los riesgos con la ayuda de diversos estándares, minimizándolos a un nivel aceptable, es por eso que se recomienda mantener un constante control de todos los procesos de seguridad.

El trabajo eficaz de la seguridad de los sistemas de información es un aspecto primordial para defender a las organizaciones de los riesgos e inseguridades que pueden dañar de forma considerable los sistemas de información (UNIT, 2005).

En resumen, la seguridad de la información es el conjunto de medidas preventivas y reactivas que las organizaciones y los sistemas tecnológicos implementan para proteger sus datos mediante controles, procedimientos y políticas que buscan la confidencialidad e integridad de dicha información.

- **Confidencialidad**
  Acceso a la información, únicamente a individuos que cuenten con la debida autorización, impidiendo la divulgación o acceso a personas o sistemas no autorizados.
- **Disponibilidad**
  Cualidad de la información de mantenerse a disposición de personas o aplicaciones autorizadas, en el momento que la requieran.
- **Integridad**
  Particularidad que mide la capacidad de un sistema para resistir ataques tanto accidentales como intencionados contra su seguridad.(Pressman, 2002).

2.3 Riesgos

La gestión de riesgos es de suma importancia cuando se habla de seguridad de la información, es por aquellos que los controles en la Norma ISO 27001 trata de mitigar al máximo los riesgos que se puedan presentar en la gestión de la información, sugiriendo se deba seleccionarlos en base al resultado de un análisis de riesgos al que está expuesta la compañía.

2.3.1 Concepto de Riesgo

Riesgo es el suceso donde una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información o grupo de ellas (SGS, 2013).

2.3.2 Evaluar los riesgos de la seguridad de la información

La gestión de riesgos en la seguridad de la información requiere una valoración correcta y sobre todo un método de tratamiento en el riesgo que puede incluir una estimación del costo con respecto al beneficio. De la misma forma los requerimientos legales y aspectos sociales que involucran directamente la economía de las partes implicadas.

2.3.3 Análisis del riesgo

El propósito de la identificación del riesgo es fijar que podría suscitarse cuando se presente una potencial pérdida, consecuentemente llegar a advertir el cómo, dónde y por qué podría ocurrir esta pérdida, para lo cual se debe iniciar con la identificación de los activos, amenazas, controles existentes y vulnerabilidades (INCONTEC, 2008).

2.3.4 Proceso de gestión del riesgo

Como se puede ver en la Fig. 1, la comunicación y consulta son de caminos bidireccionales con el hecho propio de establecer, evaluar y tratar los riesgos que juntamente con el adecuado monitoreo y revisión se podría llegar a establecer claramente cuáles son los conflictos y poder tenerlos controlados para evitar que puedan desencadenar una acción que ponga en riesgo la información y por ende las operaciones de la empresa.

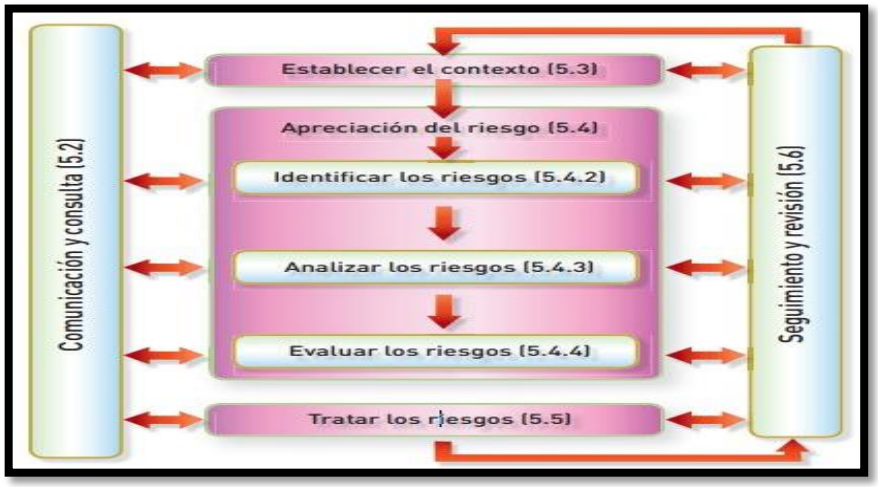


Figura 1: Proceso de gestión del riesgo (UNE-ISO 31000)

La aplicación de un proceso de gestión del riesgo en la seguridad de la información puede satisfacer diversos enfoques mediante los cuales se puede implementar exitosamente en una organización. La organización debe utilizar cualquier enfoque que se acomode mejor a sus circunstancias del proceso (INCONTEC, 2008).

2.3.5 En un SGSI se han establecido los siguientes procesos:

- **Planificar**

  Establecimiento en la valoración del riesgo, el desarrollo del plan de tratamiento del riesgo y la aceptación del mismo.

- **Hacer**

  Se implementan acciones correspondientes y controles que son necesarios para reducir el riesgo hasta un nivel aceptable

- **Verificar**

  Determina la necesidad de revisiones en las valoraciones del tratamiento del riesgo a la luz de los incidentes y los cambios en las circunstancias.

- **Actuar**

  Se lleva a cabo las acciones que son ineludibles, incluyendo la aplicación adicional del proceso de gestión del riesgo en la seguridad de la información.

El siguiente gráfico resume las actividades de gestión de riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso del SGSI:

Figura 2: Proceso de gestión del riesgo (Deming 1989)

2.3.6 Principios de gestión del riesgo.

Una de las representaciones para identificar los riesgos es mediante el siguiente gráfico en el cual, para poder tomar acciones en contra de ellos, se debe identificar los riegos según corresponda su grado de probabilidad de ocurrencia y la consecuencia que este acarrearía.

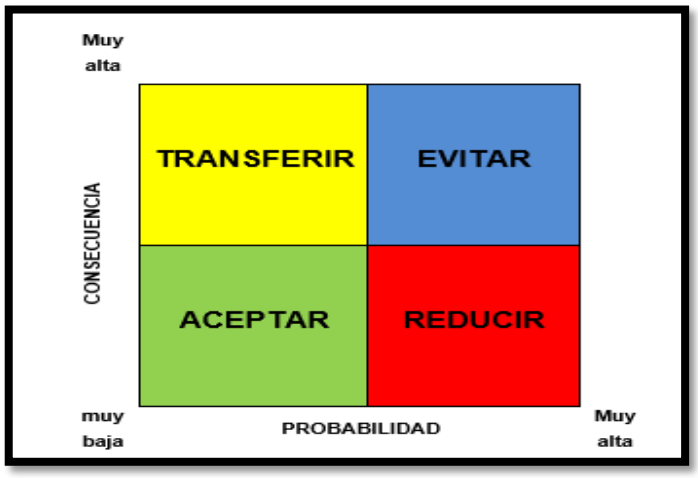


Figura 3: Principios de gestión del riesgo (SGS, 2013)

Los cuadrantes mostrados en la Figura 3 se describen a continuación:

- **Evitar:**

  Se debe impedir de cualquier manera, debido a que la probabilidad y consecuencia son muy penetrantes, si no se lo hace el riesgo se puede convertir en una gran amenaza.

- **Transferir:**

  Es un riesgo controlable, la consecuencia es alta pero la probabilidad baja, aun así, no se debe desatenderla.

- **Reducir:**

  Riesgo manejable, la probabilidad es alta, pero la consecuencia es baja.

- **Aceptar:**

  El trabajo con estos riesgos es mantenerlos en este cuadrante, donde se puede gestionar y monitorear sin entorpecer los procesos.

2.3.7 Clasificación de los activos.

Al ser uno de los activos más importantes, de acuerdo a los lineamientos de seguridad de cada organización, la información debe ser definida y valorada. Los activos han sido clasificados de la siguiente manera:

Figura 4: Clasificación de Activos (SGS, 2013)

2.3.8 Criterios Básicos de la gestión del riesgo

Una vez reconocidos y valorados los riesgos se puede tomar medidas para reducir la exposición al riesgo. Tratar un riesgo supone básicamente actuar sobre dos posibles líneas:

- **Plan de mitigación del riesgo**, efectuar acciones para reducir la probabilidad de que un riesgo se materialice.
- **Plan de contingencia**, plasmar acciones para prepararse ante la ocurrencia del riesgo y reducir el impacto que este riesgo tiene en el proyecto.

Criterios de evaluación del riesgo

Es respetable desarrollar criterios para la evaluación del riesgo con el fin de determinar el riesgo en la seguridad de la información de la organización, teniendo en cuenta los siguientes aspectos:

- Valorar el impacto en el negocio que podría resultar de un fallo de seguridad, teniendo en cuenta las consecuencias de una pérdida de confidencialidad.
- Ajustar la posibilidad de que se produzca el fallo de seguridad en función de las amenazas y vulnerabilidades, al mismo tiempo los impactos asociados.
- Considerar todo los niveles de riesgo
- Determinar si el riesgo es aceptable o requiere tratamiento usando los criterios de aceptación de riesgos establecidos. (ISO27000.es, 2005)

Criterios de impacto

Para cada criterio se deben concebir áreas de impacto, es decir, condiciones de cómo la organización se verá afectada por algún tipo de incidente de seguridad.

El impacto puede ser alto, medio o bajo, y esto deberá ser definido por el personal delegado de generar los criterios de medición del riesgo.

En la siguiente imagen se muestra un ejemplo de un área de impacto para los criterios de Reputación y confianza del cliente:

Área de impacto	Bajo	Moderado	Alto
Afectación a la imagen de la organización	La información relacionada con incidente de seguridad se conoce dentro del área de TI.	La información relacionada con incidente de seguridad se conoce dentro de la organización.	La información relacionada con incidente de seguridad se conoce públicamente.

Figura 5: Ejemplo de Área de Impacto (MENDOZA, 2014)

Considerando los siguientes aspectos:

- Nivel de clasificación de los activos de información afectados.
- Huecos en la seguridad de la información
- Operaciones malogradas.
- Pérdida del negocio y del valor financiero.
- Trasformación de planes y fechas límites.
- Incumplimiento de los requisitos legales, reglamentarios o contractuales.

Criterios de la aceptación del riesgo

Hay que recordar que los riesgos de seguridad de la información son peligros de negocio y sólo la Dirección puede tomar medidas sobre su aceptación final en cada revisión y/o acciones de tratamiento.

El riesgo residual es el que queda, aún después de haber aplicado controles (el "riesgo cero" no existe prácticamente en ningún caso). (ISO27000.es, 2005)

Se debería considerar los siguientes aspectos:

- Los criterios de aceptación del riesgo pueden incluir pasos múltiples, con un nivel de riesgo deseable por encima de este nivel y en circunstancias definidas.
- Pueden expresarse como una relación entre el beneficio estimado y el riesgo estimado.
- Se pueden aplicar a diversas variedades de riesgos.
- Pueden incluir requisitos para un tratamiento adicional en el futuro, es decir se puede tomar acciones que reduzcan el riesgo hasta un nivel aceptable en un periodo definido de tiempo.

Finalmente, se pueden delinear de acuerdo con la expectativa de duración que se tenga, para lo cual se debería considerar elementos tales como: criterios

del negocio, aspectos lógicos y sistemáticos, operaciones, tecnología, finanzas, factores sociales y humanitarios (INCONTEC, 2008).

2.3.9 El alcance y límites del riesgo

La organización debe asegurarse que todo el personal dentro del alcance del SGSI dispone de responsabilidades determinadas para desempeñar las tareas requeridas para:

- Establecer competencias necesarias del personal que realiza trabajos que afectan el SGSI
- Facilitar acciones concretas para el personal competente y satisfacer dichas necesidades
- Apreciar la eficacia de las acciones tomadas y mantener los registros de habilidades, experiencia y calificaciones.

Al definir el alcance y los límites, la organización debería considerar la siguiente información:

- Objetivos estratégicos de negocio y políticas de la organización.
- Procesos del negocio en cada dependencia.
- Funciones, estructura y nivel jerárquico de la organización.
- Requisitos legales y contractuales que sean aplicables a la organización.
- Políticas eficientes de seguridad de la información dentro de la organización.
- Enfoque a nivel macro de la organización dirigida a la gestión del riesgo.
- Activos valederos de información.
- Ubicación de la organización y características geofísicas.
- Restricciones reales que afectan a la organización.

Si existiera alguna exclusión del alcance, esta o estas deberían ser suministradas por la misma organización (INCONTEC, 2008).

2.3.10 Identificación del riesgo

El propósito de la identificación del riesgo es determinar los sucesos que cause una pérdida potencial, y llegar a comprender el cómo, dónde y por qué podría ocurrir esta pérdida. Se debería recolectar datos de entrada para la actividad de estimación del riesgo.

Al momento de identificar los riesgos se debe:

- Identificar aquellos activos de información que tienen algún valor para la organización que están dentro del alcance del SGSI y a sus responsables directos.
- Equilibrar las amenazas relevantes asociadas a los activos identificados
- Empatar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas
- Reconocer el impacto que podría suponer una pérdida de confidencialidad, integridad y disponibilidad para cada activo. (ISO2700.ES, 2012)

2.3.11 Identificación de las vulnerabilidades

Vulnerabilidades:

Debilidad del sistema informático que puede ser utilizada para causar un daño. Pueden emerger en cualquiera de los elementos de un computador, tanto en el hardware cómo en el software.

Al ser identificados los puntos débiles, será factible dimensionar los riesgos a los cuales el ambiente está expuesto y así finiquitar las medidas de seguridad apropiadas para su inmediata corrección.

Amenazas:

En un sistema informático es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.

Como ejemplos claros de amenaza están los ataques por parte de personas, al igual que los desastres naturales que puedan afectar al computador. También hay que considerar los fallos cometidos por los usuarios al utilizar el sistema o los fallos internos tanto del hardware o cómo del software. (Roldán, 2012).

Los activos reales están constantemente sometidos a amenazas que pueden colocar en riesgo la integridad, confidencialidad y disponibilidad de la información. Estas amenazas son latentes y siempre existirán.

Uno de los objetivos de la seguridad de la información es impedir que las amenazas detonen puntos débiles y afecten alguno de los principios básicos de la seguridad de la información como la integridad, disponibilidad y confidencialidad, causando daños al negocio de las empresas. (Jaimes, 2009).

En los sitios de la organización en las cuales se pueden identificar las vulnerabilidades son las siguientes:

- Organización.
- Procesos y rendimiento.
- Rutinas de gestión.
- Personal.
- Ambiente físico.
- Configuración del sistema de información.
- Hardware, software o equipos de comunicaciones.
- Dependencias de partes externas.

La presencia de una o varias vulnerabilidades no causa daño por sí misma, dado que es necesario que haya una amenaza presente para detonarla. Una vulnerabilidad que no dispone de una amenaza incurre en la implementación de un control, pero si es necesario tomar medidas y monitorearlas para comprobar los cambios.

Por el contrario, una amenaza que no tiene una vulnerabilidad correspondiente puede no resultar un riesgo (INCONTEC, 2008).

2.3.12 Reducción del Riesgo

La mitigación de los riesgos se logra a través de la implementación de medidas de protección, que basados en los resultados se toma medidas correctivas para no dar lugar a ningún tipo de sesgo.

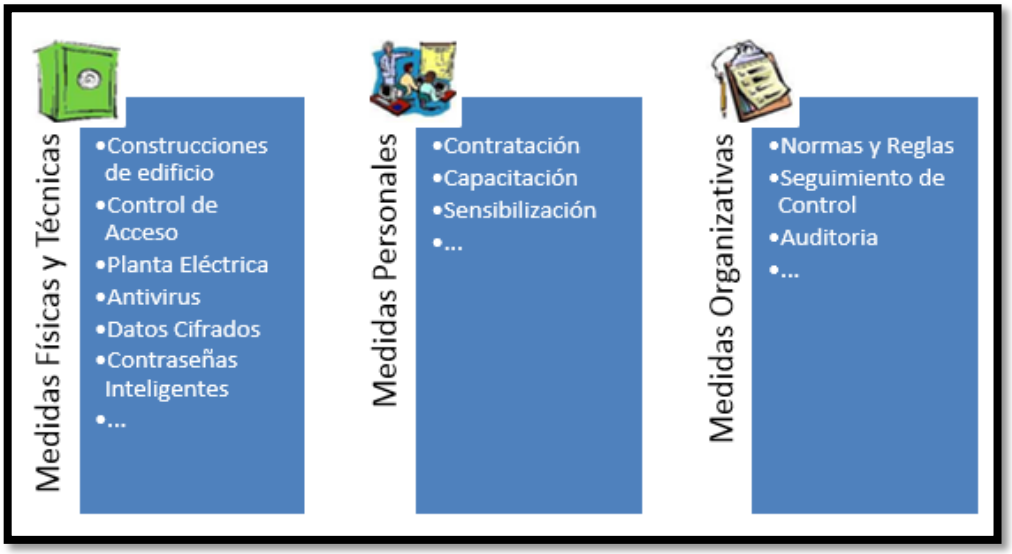


Figura 6: Reducción del Riesgo

Considerando en toda ocasión que la implementación de medidas de protección se encuentra directamente proporcionadas con inversiones de recursos financieros y operativos, es más que innegable, que las medidas para

evitar un daño resultarán mucho más costosas y complejas que aquellas que mitigan un solo daño.

Para que las medias resulten plenamente exitosas, es esencial que siempre se verifique su factibilidad, es decir que técnicamente funcionan y cumplen su propósito. Es indispensable que se encuentren respaldadas y sobre todo aprobadas por la Coordinación.

También significa que deben ser diseñadas de tal manera, que no paralizan u obstaculizan los procesos operativos porque deben apuntalar el cumplimiento de la misión, mas no impedirlo.

Otro punto relevante es el indicador humano, basados en el propósito e importancia de sus capacitadas para el buen uso, de tal manera, que las identifiquen como una necesidad institucional y no como una imposición laboral.

Debido a que la implementación de las medidas no es una labor aislada, sino un proceso continuo, su manejo y mantenimiento debe estar integrado en el funcionamiento operativo institucional, preservado por normas y reglas que regulan su aplicación, control y las sanciones en caso de incumplimiento. (Erb, 1999).

2.3.13 Monitoreo y revisión de los factores de riesgo

La organización deberá:

- Ejecutar procedimientos de monitorización y revisión para:
    - Detectar con tiempo los errores en los resultados generados por el procesamiento de la información.
    - Identificar huecos e incidentes de seguridad.

- Ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos garantizan la seguridad de la información.
- Prevenir eventos e incidentes de seguridad mediante el uso de indicadores
- Estipular si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

- Inspeccionar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI.
- Medir la efectividad de los controles para verificar que se cumplan al pie de la letra los requisitos de seguridad.
- Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, asumiendo posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio.
- Es saludable realizar periódicamente auditorías internas del SGSI en intervalos planificados para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001:2005, el entorno legal y los requisitos y objetivos de seguridad de la organización, están implementados y mantenidos con eficacia y tienen el rendimiento esperado.
- Examinar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo las adecuadas y posibles mejoras en el
- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y escrutinio.
- Rastrear acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI. (ISO27000.es, 2005).

Las organizaciones deberían atestiguar el continuo monitoreo de los siguientes aspectos:

- Activos desconocidos que se han incluido en el alcance de la gestión de riesgo.
- Transformaciones necesarias de los valores en los activos que suelen suscitarse por cambios en los requisitos de los negocios.
- Eventos que podrían estar activos tanto fuera como dentro de la organización y que no se han apreciado.
- Probabilidad de que nuevas vulnerabilidades permitan que las amenazas se vuelvan una realidad.
- Flaquezas identificadas para determinar aquellas que se exponen a nuevas amenazas o que vuelven a acontecer.
- El incremento e impacto producido en las amenazas evaluadas, donde las vulnerabilidades y los riesgos en conjunto dan como deducción un nivel inaceptable.
- Constantes incidencias en la seguridad de la información.

Las nuevas amenazas, vulnerabilidades o cambios en la probabilidad o las consecuencias pueden incrementar los riesgos valorados previamente como riesgos bajos (INCONTEC, 2008).

2.4 Normas ISO 27000

La información es un activo trascendental para el éxito y la continuidad en el mercado de cualquier organización. El fortalecimiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

Para la correcta gestión de la seguridad de la información, es imperioso implantar un sistema que aborde esta tarea de una forma metódica,

documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

ISO/IEC 27000 es un conjunto de estándares desarrollados o en fase de desarrollo por la ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que suministran un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización sea pública o privada, grande o pequeña (Neira, 2012).

2.4.1 Origen

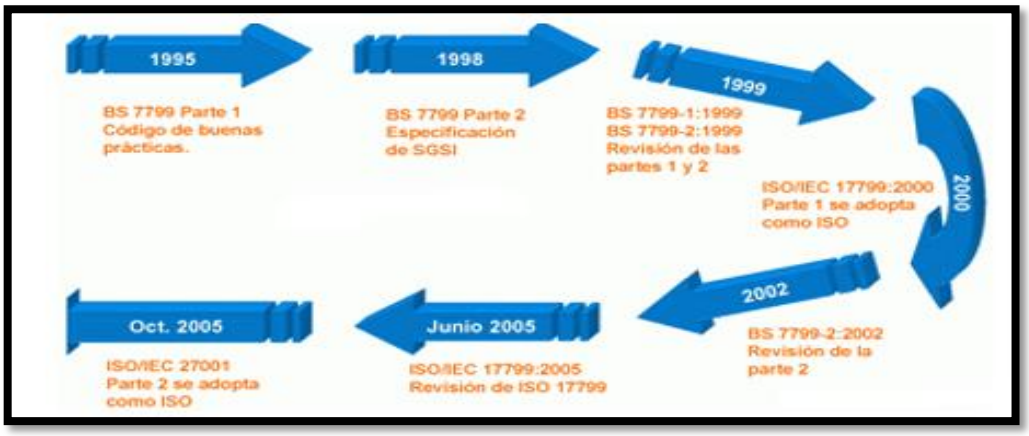


Figura 7: Historia de ISO 27001. (ISO2700.ES, 2012)

Desde el año 1901 y como principal entidad de normalización a nivel mundial, BSI (British Standards Institution, la organización británica equivalente a AENOR en España) es garante de la publicación de importantes normas como:

- 1979 Anteriormente, Publicación BS 5750 - Actualmente ISO 9001
- 1992 Anteriormente, Publicación BS 7750 - Actualmente ISO 14001
- 1996 Anteriormente, Publicación BS 8800 - Actualmente OHSAS 18001

La norma BS 7799 de BSI surge por primera vez en 1995, con el objeto de aportar a cualquier empresa británica o no, un conjunto de buenas prácticas para la gestión de la seguridad de su información.

El primer fragmento de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. En el segundo fragmento (BS 7799-2) implanta los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Los dos fragmentos de la norma BS 7799 se inspeccionaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En el año 2005, con un aumento de más de 1700 empresas certificadas en BS7799-2, el esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó.

Esta última norma ISO17799 se renombra como ISO 27002:2005 el 1 de Julio de 2007, conservando el contenido, así como el año de publicación de la revisión formal (ISO27000.es, 2005).

2.4.2 Definición de las normas ISO 27000

Similar a otras normas la serie ISO 27000 es un linaje de estándares internacionales que tiene niveles de numeraciones reservadas por ISO que van de la 27000 a 27019 y de 27030 a 27044.

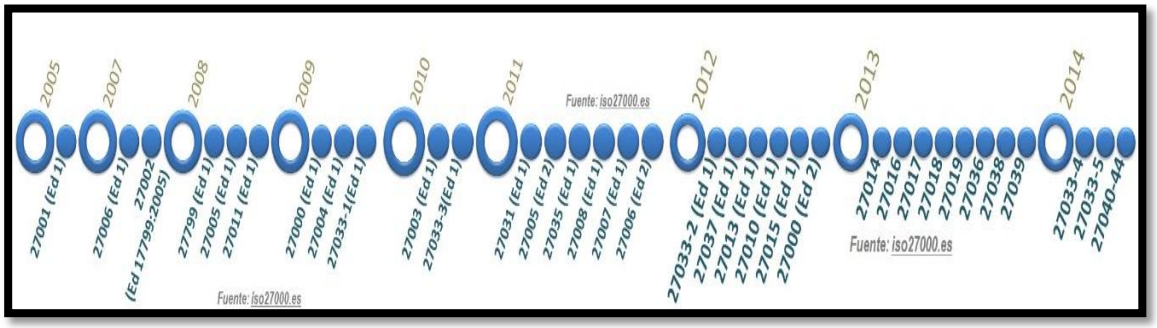


Figura 8: Evolución ISO 27000. (ISO27000.es, 2005)

ISO 27000

Publicada el 1 de mayo de 2009, examinada con una segunda edición el 01 de diciembre de 2012 y una tercera edición de 14 de enero de 2014, ésta norma proporciona una visión universal de las normas que componen la serie 27000, enseñando para cada una de ellas su alcance de actuación y el propósito de su publicación.

Acumula todas las definiciones para la serie de las normas 27000 y aporta las bases para explicar del porque es importante la formación de un SGSI. Un preámbulo a los Sistemas de Gestión de Seguridad de la Información explica con una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI.

ISO 27001

Publicada el 15 de octubre de 2005, examinada el 25 de septiembre de 2013 declara la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información.

Tiene su comienzo en la BS 7799-2:2002 de la cual ya quedó anulada y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones. A pesar del desconsuelo, al no ser obligatoria la implementación de todos los controles, la organización deberá argumentar fuertemente la no aplicabilidad de los controles no implementados. (ISO27000.es, 2005)

ISO 27002.

Desde el 1 de Julio de 2007, su nuevo nombre ha sido ISO 17799:2005, manteniéndolo hasta el 2005 como año de edición. Es una pauta de buenas prácticas que describe los objetivos de control como también controles recomendables en cuanto a seguridad de la información. Sujeta 39 objetivos de control y 133 controles, agrupados en 11 dominios.

En la actualidad, este estándar se encuentra en periodo de revisión en el subcomité ISO SC27, con fecha prevista de publicación de la segunda edición en mayo de 2014 (ISO27000.es, 2005).

ISO 27003.

Publicada el 01 de febrero de 2010. No certificable. Es una guía que se centraliza en los aspectos críticos que son necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005.

Puntualiza el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de los planes de implementación, así como el proceso de obtención de la aprobación por la dirección para implementar un SGSI.

ISO 27004

Publicada el 15 de diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y métodos de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001, al mismo tiempo, esta norma proporciona representaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información.

ISO 27005

Anunciada en segunda edición el 1 de junio de 2011 (primera edición del 15 de junio de 2008). No certificable. Aporta directrices para la gestión del riesgo en la seguridad de la información. Apuntala los conceptos generales especificados en la norma ISO/IEC 27001:2005 y se encuentra diseñada para colaborar con la seguridad de la información basada en un enfoque de gestión de riesgos.

Esta norma es adecuada para los directores y el personal involucrado en la gestión del riesgo en la seguridad de la información y también para los segmentos externos que dan soporte a dichas actividades.

Igualmente, apoya los conceptos universales especificados en la norma ISO/IEC 27001:2005 y está delineada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos (INCONTEC, 2008).

ISO 27006

Describe los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada es decir, ayuda a desentrañar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma. (ISO2700.ES, 2012).

ISO 27007

Publicada el 14 de noviembre de 2011. No certificable. Es una guía de auditoría de un Sistema de Gestión de Seguridad de la Información, como mejoramiento a lo especificado en ISO 19011.

ISO 27031

Norma publicada el 01 de marzo de 2011. No es certificable. Es una guía de soporte para la adecuación de las tecnologías de información y comunicación de una organización para la continuidad del negocio.

ISO 27032

Publicada el 16 de Julio de 2012. Provee orientación para la mejora del estado de la seguridad cibernética donde extrae los aspectos únicos de esa actividad y de sus dependencias en otros dominios, resumidamente brinda protección de infraestructura de tipo crítica (CIIP).

Reviste prácticas de seguridad a nivel básico para los interesados en el ciberespacio. Esta norma establece un diseño general con explicación de la relación entre la ciberseguridad y otros tipos de garantías permitiendo a las partes interesadas que colaboren en la solución de problemas en ciberseguridad.

ISO 27034

Norma diligente basada en la seguridad con aplicaciones informáticas, y estable las siguientes 6 partes:

27034-1: Conceptos habituales.
27034-2: Marco normativo de la estructura.
27034-3: Proceso de gestión de seguridad en aplicaciones.
27034-4: Validación de la seguridad en aplicaciones.
27034-5: Distribución de los datos, protocolos y controles de seguridad de aplicaciones.
27034-6: Guía de seguridad para aplicaciones de uso definido.

2.4.3 Estándar ISO/IEC 27001

Generalidades

ISO 27001 es una norma internacional presentada por la Organización Internacional de Normalización (ISO) y detalla el cómo se debe gestionar la seguridad de la información en una empresa. El escrutinio más reciente de esta norma fue publicada en el año 2013 donde su nombre completo es ISO/IEC 27001:2013.

ISO 27001 puede ser implementada en cualquier tipo de organización, redactada por los mejores especialistas del mundo en el tema proporcionando una metodología para implementar la gestión de la seguridad de la información en una organización. De igual forma, permite que una empresa sea legitimada;

esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido efectuada en ésa organización en cumplimiento con la norma ISO 27001.

ISO 27001 se ha trasformado en la principal norma a nivel mundial para la seguridad de la información y considerables empresas han certificado su cumplimiento, aquí se puede observar el aumento de certificaciones en los últimos años:

Figura 9: Encuesta ISO sobre certificaciones de la norma para sistemas de gestión. (Rhand Leal, 2012)

Enfoque basado en procesos

Esta norma suscita la adopción de un enfoque basado en procesos, para hacer funcionar eficazmente una organización, de lo cual se debe identificar y gestionar muchas actividades. Se puede considerar como un proceso cualquier actividad que use recursos y cuya gestión permita la alternativa de entradas en salidas.

La diligencia de un sistema dentro de una organización, junto con la identificación e interacciones entre estos procesos y su gestión se puede denominar como una perspectiva basada en procesos.

Esta norma adopta el modelo de procesos o ciclo de Deming “PHVA o PDCA” (Planificar-Hacer-Verificar-Actuar o Plan-Do-Check-Act), que se utiliza para combinar todos los procesos del sistema de Gestión de Información (SGS, 2013).

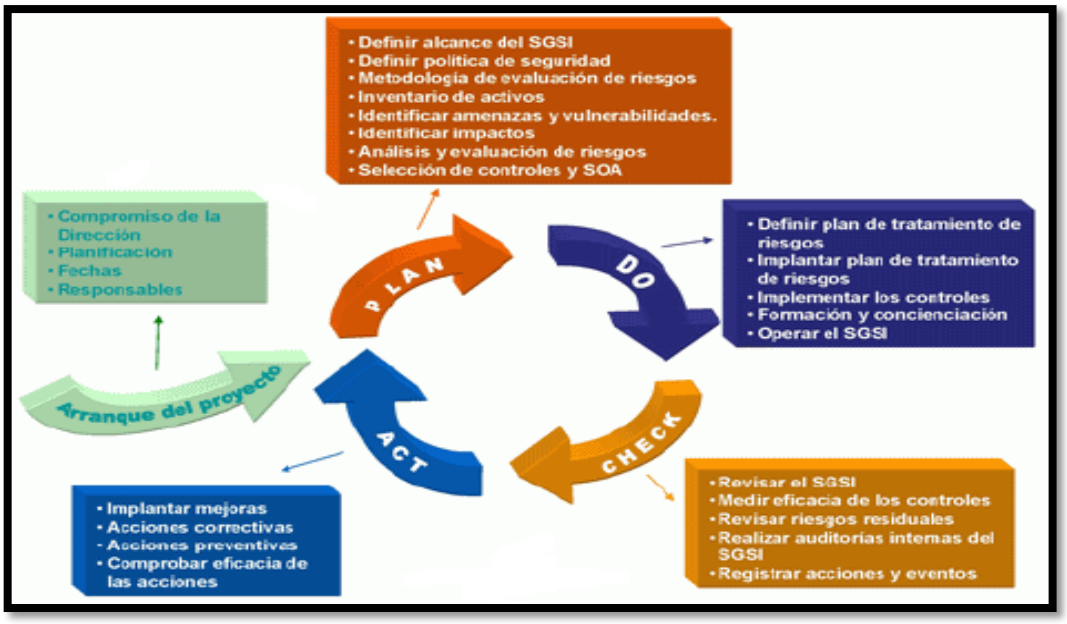


Figura 10: Ciclo de adaptación de la Norma (SGS, 2013)

Como se puede comprender en la figura 10 el ciclo PHVA, está compuesto por los siguientes términos que significan:

- **Planear (P):**

  Consiste en el establecimiento de políticas, objetivos, procesos y metas oportunas para formalizar el riesgo y mejorar la seguridad de la información con el único fin de atribuir indicadores de resultados y establecer el mejor camino para alcanzar las metas propuestas por una organización.

- **Hacer (H o D):**

  Ejecución estricta de las tareas de la forma prevista en el procedimiento y en la recolección con los datos para la verificación del proceso.

- **Verificar (V o C):**

  Se toma en cuenta basados en los datos recolectados la ejecución para poder hacer la comparación compara con la meta planificada.

- **Actuar (A):**

  Etapa en la cual el usuario detectó desvíos y desplegará soluciones de modo que el problema no se repita, es decir tomar las acciones correctivas y preventivas con base en los resultados de la auditoría interna, así poder finiquitar la mejora continua del SGSI (Universidad de Colombia, 2012).

Dominios ISO27001

- **Generalidades**

Tiene como objetivo la vigilancia de la información de una organización impidiendo que ésta se pierda, proporcionando continuidad de los servicios prestados en situaciones de riesgo.

Figura 11: Dominios ISO27001 (SGS, 2013)

- **Políticas de Seguridad**

Un documento con terminología política, es aquel que pronuncia una intención e instrucción global en la manera que formalmente ha sido expresada por la Dirección de la organización.

El contenido de las políticas en contexto se basa en la interoperabilidad de una organización y suelen ser consideradas en su redacción para los fines adoptados, es decir, implícitamente alcanzar los objetivos procedentes de niveles más superiores como lo es el obligado cumplimiento del sector al que pertenece la organización.

Una estructura típica de los documentos de políticas suelen ser:

- Resumen: Visión general de una extensión, una o dos frases que pueden aparecer fusionadas con la introducción.
- Introducción: Breve explicación de la temática principal en la política institucional.
- Ámbito de aplicación: Delineación de los departamentos, áreas o actividades de una organización donde son afectadas por las políticas de la empresa. Cuando es relevante, se mencionan otras políticas a las que se pretende dar cobertura inmediata.
- Objetivos: Representación de la intención global de la política interna.
- Principios: Diseño de las reglas que conciernen a acciones o decisiones para alcanzar los objetivos. En cualesquier caso puede ser de suma utilidad identificar previamente los procesos claves para consecuentemente identificar las reglas de operaciones en los procesos.
- Responsabilidades: Descripción de quién es garante de qué trabajos se cumplirán para delimitar los requisitos de la política empresarial.
- Resultados claves: Descripción de los resultados sumamente relevantes para las actividades de la organización que se obtienen cuando se cumplen los objetivos.

- Políticas relacionadas: Delineación de otras políticas relevantes para el cumplimiento de los objetivos, prácticamente se indican los detalles adicionales en relación a temas específicos.

La política de alto nivel habitualmente conexa con el sistema de gestión para la seguridad de la información (SGSI) suele estar apoyada por políticas de bajo nivel, para la respectiva clasificación de la información, seguridad física y ambiental.

Partiendo del principio típico en seguridad, cada organización debería detectar las necesidades de los usuarios y valorar los controles necesarios que fundamenten las políticas aplicables, aplicando la mejor estructura y relaciones entre ellas para su buena gestión.

- **Organización.**

El objetivo es establecer la administración de la seguridad de la información como parte fundamental de los objetivos y actividades de la organización.

Para ello se debería puntualizar formalmente un ámbito de gestión para efectuar tareas como la aprobación de las políticas de seguridad, coordinación de la implementación de seguridad y la asignación de funciones concatenadas con las responsabilidades.

Para una actualización adecuada en materia de seguridad se debería contemplar la insuficiencia en las fuentes de conocimiento para el asesoramiento, cooperación y colaboración en materia de seguridad de la información.

Los resguardos físicos de las organizaciones son cada vez más inapreciables por las actividades mismas de la empresa, donde se requiere por parte del personal se acceda a información desde el exterior en situaciones de movilidad sean éstas temporales o permanentes.

En estos casos se considera que la información podría ponerse en riesgo si el acceso se produce en el marco de una inadecuada administración, por lo que se establecerán las medidas adecuadas para el resguardo de la información.

- **Recursos Humanos**

El objetivo es concientizar e informar al personal acerca de las medidas de seguridad que afectan al desarrollo de las diversas funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad.

Es ineludible reducir los riesgos de errores humanos, comisión de actos ilícitos, uso inadecuado de instalaciones y recursos no autorizado de la información, junto a la definición de políticas con sanciones que se aplicarán en caso de incumplimiento.

Se requiere explicar las responsabilidades en materia de seguridad en la etapa de reclutamiento del personal e incluirlas en los acuerdos a ser firmados, así como garantizar que los usuarios estén al corriente de las amenazas en materia de seguridad de la información, y se encuentren capacitados para respaldar sus tareas normales.

Suele ser responsabilidad del departamento de Recursos Humanos incluir las situaciones relativas a la seguridad de la información en las delineaciones de puestos de cada uno de los empleados, de la misma manera informar a todo el personal que ingresa de todas sus obligaciones respecto al estricto cumplimiento de la Política de Seguridad de la Información puntualizando los compromisos de confidencialidad respecto a las necesidades presentes en seguridad.

El ente encargado del área jurídica, es quien participa en la confección del compromiso de confidencialidad a ser firmar por los empleados y terceros que desplieguen las funciones en la entidad.

- **Activos**

El objetivo del presente dominio es que la organización posea conocimientos precisos sobre los activos que posee como parte significativa de la administración de los riesgos.

Algunos ejemplos de activos sobresalientes son:

- Recursos de información: Bases de datos y archivos, expediente de sistemas, manuales de usuario, material para capacitación, procedimientos de ámbito operativo, planes de continuidad con información registrada.
- Recursos de software: Software de aplicaciones, sistemas operativos, herramientas de desarrollo y divulgación de contenidos.
- Activos físicos: Equipamiento netamente informático que abarca los procesadores, monitores, ordenadores, módems, equipos de comunicaciones, medios magnéticos, entre otros.
- Servicios: Productos informáticos y de comunicaciones, utilitarios generales que abarca la calefacción, iluminarias, energía eléctrica.

Los activos de información deben ser catalogados de acuerdo a la comprensión y criticidad de la información que contiene el objeto de señalar cómo ha de ser procesada y preservada dicha información.

Las pautas de clasificación deben avistar el hecho de que un ítem determinado no necesariamente debe mantenerse invariable por siempre. Se debería considerar la suma de categorías a ser definidas para la clasificación,

dado que los esquemas complejos pueden tornarse complejos o simplemente ser poco prácticos.

- **Control de Accesos**

Controlar el acceso por medio de un sistema de prohibiciones y al mismo tiempo excepciones hacia la información como pedestal de todo sistema de seguridad informática.

Para disuadir el acceso no autorizado a los sistemas de información se debería efectuar ordenamientos formales para examinar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, éstos deben estar visiblemente argumentados y comunicados.

Las operaciones comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, como es el registro inicial de nuevos usuarios hasta llegar a la privación final de usuarios que ya no necesiten el acceso.

La cooperación de los usuarios es fundamental para la eficacia de la seguridad, por lo tanto, es ineludible concientizar a los mismos acerca de sus responsabilidades, en particular aquellos que tienen concatenación con el uso de contraseñas y seguridad del equipamiento.

- **Cifrado**

Uso de sistemas con técnicas criptográficas para la defensa en la información con el fin de asegurar una apropiada protección de su confidencialidad e integridad.

La concentración de medidas de cifrado se debería desarrollar en base a una política sobre el uso de controles criptográficos, aún más ante el establecimiento de gestión de las claves que apoyen radicalmente la aplicación de técnicas criptográficas.

- **Seguridad Física y Ambiental**

Minimizar los riesgos de daños en las operaciones de la organización. El establecimiento de círculos de seguridad y áreas protegidas facilitan claramente la ejecución de controles de protección de las instalaciones contra los caminos físicos no autorizados.

La vigilancia de los factores ambientales de origen interno y externo permite responder el correcto funcionamiento de los equipos y minimizar las posibles interrupciones de servicio.

La información recopilada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento son susceptibles mientras no están siendo manipulados. Es por ello, que deben ser valorados primordialmente en casos en los que los equipamientos pertenecientes a la organización estén físicamente fuera del mismo o en equipamiento ajeno.

- **Seguridad Operativa**

Controlar la existencia de los procedimientos de operaciones, sobre todo el desarrollo y mantenimiento de la documentación coherente.

Como valor agregado se debería calcular el posible impacto operativo de los cambios previstos en el sistema, verificar su correcta implementación, asignando métricas de responsabilidad para permitir la segregación de los ambientes y responsabilidades en el procesamiento.

Con el objeto de evitar potenciales amenazas a la seguridad del sistema sería obligatorio monitorear las necesidades de capacidad de los sistemas en operación y maquinar las futuras demandas de desplazamiento.

El control en la realización de copias de resguardo de información permite garantizar que los tiempos de recuperación establecidos sean cien por ciento

reales evitando pérdidas de información que serán indirectamente asumibles para cada organización.

Se deberían especificar y documentar los controles para la detección y prevención del acceso no autorizado, sean estos para software malicioso y las transacciones conectados a las redes de la organización.

Finalmente, se deberá confirmar el cumplimiento de las normas, procedimientos y controles mediante auditorías técnicas como base para la monitorización del estado del riesgo en los sistemas y ante futuros descubrimientos de nuevos riesgos.

- **Seguridad en las Telecomunicaciones**

Asegurar la protección de la información que se informa por las redes telemáticas y sobre todo la protección de la infraestructura de soporte.

La gestión segura de las redes requiere de la meticulosa capacidad en realizar un flujo de datos, implicaciones legales, monitoreo y protección.

Los intercambios de información por parte de las organizaciones se deberían basar en una política formal de intercambio, así mismo deberá cumplir con cualquier legislación apreciable.

- **Adquisición, desarrollo y Mantenimiento de los sistemas de información.**

Asegurar la inclusión de controles de seguridad y total validación de los datos en la adquisición y desarrollo de los sistemas de información.

Puntualizar los procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan. Aplica a todos los sistemas informáticos que compongan cualquiera de los ambientes administrados por la organización.

- **Relaciones con Suministradores.**

Implementar manteniendo el nivel apropiado de seguridad de la información y la respectiva entrega de todos los servicios contratados en línea con los acuerdos estipulados de entrega.

La organización debe examinar la implementación de los acuerdos, monitorear su acatamiento con los estándares y manejar los cambios para ser entregados satisfaciendo los requerimientos acordados con terceras personas.

- **Gestión de Incidentes**

Garantizar que los eventos de seguridad de la información y los enflaquecimientos asociados sean comunicados de forma oportuna, tal que se apliquen acciones correctivas inmediatas en el tiempo oportuno.

Las organizaciones cuentan con innumerables activos de información, cada uno mostrado a tolerar incidentes de seguridad, por consiguiente resulta imperioso contar con la capacidad de gestión de dichos incidentes.

- **Aspectos en la Gestión de la Continuidad de Negocio**

Salvaguardar la seguridad de la información durante las fases de activación, procedimientos, desarrollo de procesos y planes para la continuidad de negocio.

Se debería constituir dentro de los procesos críticos de negocio, aquellas necesidades de gestión de la seguridad de la información prestando gran importancia a las operaciones, el personal y finalmente la logística.

Se tomará en cuenta los desastres, fallas de seguridad, pérdidas de servicio para poder desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restituir en los plazos requeridos. Deberían llevarse a cabo las pruebas pertinentes para proteger los planes actualizados, ampliar la confianza de la dirección en los planes a corto,

mediano y largo plazo, hacer hincapié en las responsabilidades bajo condiciones de desastre.

Minimizar los efectos de las potenciales interrupciones de las actividades normales de la organización que se encuentren asociadas a los desastres naturales, así proteger los procesos críticos mediante una mezcla de controles preventivos y acciones de recuperación.

- **Cumplimiento**

El diseño conjuntamente con la operación y administración de los sistemas de información están regulados por disposiciones legales y contractuales. Los requisitos normativos y contractuales pertinentes a cada sistema de información deberán estar definidos y documentados.

El objetivo es cumplir con las normativas contractuales a fin de evitar sanciones administrativas hacia la organización y empleados que incurran en responsabilidad civil o penal como consecuencia de incumplimientos.

Se debe reconocer la seguridad de los sistemas de información periódicamente a efectos de atestiguar la adecuada aplicación de la política, sobre las plataformas tecnológicas y los sistemas de información.

- **Aplicación.**

Los requisitos determinados en esta norma son genéricos y están previstos para ser adaptables a todas las organizaciones. Cualquier exclusión de controles condiciona justificarse y debe suministrarse evidencia de que los riesgos asociados han sido aceptados por las personas garantes.

Si se excluye algún control las manifestaciones de conformidad con esta norma no serán aceptables a menos que dichas exclusiones no afecten la

capacidad de la organización y la responsabilidad para entregar seguridad de la información que satisfaga los requisitos de seguridad.

- **Términos y definiciones.**

Esta norma utiliza términos y definiciones con los que se trabajará durante el desarrollo del proyecto.

- **Aceptación de riesgo:** Decisión de tomar el riesgo
- **Activo:** Objeto que tiene un valor para la organización
- **Análisis de riesgo:** Uso consecuente de la información para asemejar las fuentes y poder estimar el riesgo.
- **Confidencialidad:** Determina la condición donde la información no esté disponible ni sea relevada a individuos o procesos que no estén debidamente autorizados
- **Control:** Medios para manejar los riesgos, donde se incluyen políticas, procedimientos, lineamientos y estructuras organizacionales
- **Declaración de aplicabilidad:** Documento que relata los objetivos de controles pertinentes y aplicables para el SGSI de la organización
- **Disponibilidad:** Información de carácter accesible y utilizable por solicitud primaria de una autorizada
- **Evaluación de riesgo:** Riesgo estimado que determina la importancia en el alcance
- **Gestión de riesgo:** Actividades sistematizadas para dirigir y controlar una organización en relación con el tiempo estimado

- **Integridad:** Propiedad de proteger la exactitud y el estado de los activos de la empresa
- **Incidente de seguridad de la información:** Eventos de la información no deseados que tienen una probabilidad característica de comprometer las operaciones del negocio y puede amenazar considerablemente la seguridad de la información.
- **Lineamiento:** Representación donde se aclara qué se debería hacer y cómo para obtener los objetivos formulados.
- **Política:** Direcciones enmarcadas para expresada formalmente las directrices de la gerencia
- **Riesgo:** Combinación de la probabilidad más la concurrencia
- **Riesgo residual:** Nivel sobrante de riesgo posteriormente del tratamiento de riesgo
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información donde involucra latentemente fiabilidad
- **Sistema de seguridad de la información SGSI:** Parte del sistema que se enfoca hacia los riesgos globales de un negocio y su desenlace es establecer, revisar, mantener y mejorar competitivamente la seguridad de la información.
- **Amenaza:** Causa potencial de un incidente, el cual puede repercutir en daños a un sistema en la organización.
- **Vulnerabilidad:** Debilidad de un activo que puede ser explotada por una o más amenazas.
- **Valoración del riesgo:** Proceso global de análisis y evaluación del riesgo (SGS, 2013).

2.4.4 Estándar ISO/IEC 27002.

La ISO/IEC 17799, también denominada ISO 27002, es una pauta de buenas prácticas en la gestión de la seguridad de la información, sujeta 39 objetivos de control y 133 controles agrupados con un número de 11 dominios principales.

Alcance

Proporcionan un lineamiento general sobre los objetivos de gestión de seguridad de la información donde se deja por sentado lo que se va a realizar y lo que no se va a realizar.

	DOMINIOS	***Objetivos***	***Controles***
1	Políticas de Seguridad	1	2
2	Organización de la Seguridad de la Información	2	11
3	Gestión de Activos	2	5
4	Seguridad de Recursos Humanos	3	9
5	Seguridad Física Ambiental	2	13
6	Gestión de Comunicaciones y Operaciones	10	32
7	Control de Acceso	7	25
8	Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	6	16
9	Gestión de Incidentes de seguridad de la información	2	5
10	Gestión de la Continuidad Comercial	1	5
11	Conformidad	3	10

Figura 12: Cláusulas Objetivos y Controles de la Norma ISO 27002

El orden de las condiciones no establece su importancia, todas las condiciones pueden ser importantes, consecuentemente, cada organización que aplica este estándar debería identificar las cláusulas aplicables (ISO27000.es, 2005).

CAPÍTULO III
SITUACIÓN ACTUAL DE PRONACA

3.1 Antecedentes históricos y legales de la organización

PRONACA es el resultado de años de trabajo, perseverancia y mucha creatividad. Como empresa procesadora y comercializadora de alimentos, ha alcanzado grandes reconocimientos por la calidad de sus productos que provienen de los sectores cárnicos, agroindustrial y acuacultura.

Es una empresa ecuatoriana, que goza de confianza y aceptación dentro y fuera del país, y contribuye a perfeccionar la productividad en el ámbito agrícola e industrial. Está constituida por diferentes compañías relacionadas con la industria alimenticia y avícola, donde surgió bajo el concepto de crear una cadena de industrias que se abastezcan entre sí, permitiendo una mayor productividad y eficiencia como giro de negocio.

Sus actividades tienen como columna principal las diversas necesidades de los consumidores, conjuntamente con las exigencias donde sobresale el alto compromiso diario de sus colaboradores ante los usuarios.

Conociendo afirmadamente que es una empresa comprometida con el mejoramiento de la calidad de vida de sus consumidores, clientes y colaboradores, se trabaja profesionalmente todos los días en la elaboración de productos confiables, al mismo tiempo, ofrece miles de fuentes de trabajos dignos y apoya al desarrollo sustentable de las zonas rurales del Ecuador. Es decir, la empresa posee un ético enfoque de equilibrio entre las relaciones PROVEEDOR (ARP) EMPRESA (GCSI) – CLIENTE (ARC).

3.2 Historia.

En 1957 se constituye la compañía INDIA, quienes es la antecesora del grupo, dedicada a la importación y distribución de insumos agropecuarios y de artículos para la industria textil.

En 1958 en la hacienda La Estancia ubicada en Puembo da sus primeros pasos con la realización de huevos comerciales y la venta de pollitas importadas. Para 1965 se constituye la empresa INCA e Incubadora Nacional C.A., quien fue la primera empresa en el Ecuador en formalizar el proceso de incubación de manera tecnificada utilizando personal altamente calificado, posteriormente en el mes de agosto nacen los primeros pollitos nacionales y con ello se termina la importación.

Figura 13: INDIA en sus inicios

En 1974 surge la compañía INDAVES, con el objetivo de producir únicamente huevos de manera comercial. En 1979 se funda la Procesadora Nacional de Aves C.A., PRONACA donde prepara grandemente procesos de investigación para el desarrollo y producción de semillas tanto de maíz como de arroz.

En los 80s inicia el trabajo con la integración de aves, lo cual acertadamente da un mayor impulso a los ingresos. Inmediatamente se construye Avandina, la

primera granja de pollos en la provincia de Santo Domingo de los Tsáchilas donde se consolidan las actividades de producción y comercialización.

Al mismo tiempo, inicia la diversificación con otros tipos de alimentos dando paso a la instauración de Comestibles Nacionales C.A., COMNACA, que produce conservas bajo la marca GUSTADINA. Al mismo tiempo nace INAEXPO para la producción de palmito cultivado.

1990s Comienzan las operaciones en Bucay, con la creación de la Fundación San Luis, la dirige estratégicamente PRONACA para obtener un desarrollo de proyectos sociales y comunitarios que sean sostenibles y sustentables al mismo tiempo.

En el 2000 En el nuevo siglo se consolida la venta de arroz empacado bajo la marca GUSTADINA.

Figura 14: Inicio-Creación de la Compañía

El negocio de palmito se expande con la producción y comercialización a Brasil y nace INACERES de la asociación estratégica de INAEXPO con la brasileña AGROCERES.

PRONACA construye un complejo industrial en Durán y Guayas, donde se encuentra su tercera planta de producción de alimentos, balanceados y piladora de arroz, ambas plantas equipadas con la más alta tecnología en cada campo.

Se implantan avances tecnológicos muy considerables en todas las plantas de procesamiento, las mismas que alcanzan el certificado de inocuidad alimentaria HACCP.

Para el 2009 PRONACA inaugura en la ciudad de Guayaquil el nuevo Centro de Distribución, con instalaciones tecnológicas y sistemas logísticos avanzados que permitieron continuar con el fortalecimiento de la matriz productiva del Ecuador.

Actualmente, cuenta con 109 centros de operaciones a Nivel Nacional: Edificio Inverna (oficina principal) Granjas, Incubadoras, Centros de Distribución, Plantas de Proceso, Oficinas Regionales, Almacenes y Unidades Educativas. Más de 7.500 colaboradores directos.

Figura 15: Planta de conservas COMANA, INAEXPO

Finalmente, el pequeño grupo de emprendedores de hace 50 años se han transformado en una legión de miles de ecuatorianos comprometidos que se encuentran trabajando con un enfoque ético sobre valores y principios invariables, distribuyendo productos a todas las familias del país.

3.3 Localización

PRONACA cuenta con 109 centros de operación en el país: Edificio Inverna (oficina principal) Granjas, Incubadoras, Centros de Distribución, Plantas de Proceso, Oficinas Regionales, Almacenes y Unidades Educativas. Más de 7.500 colaboradores directos.

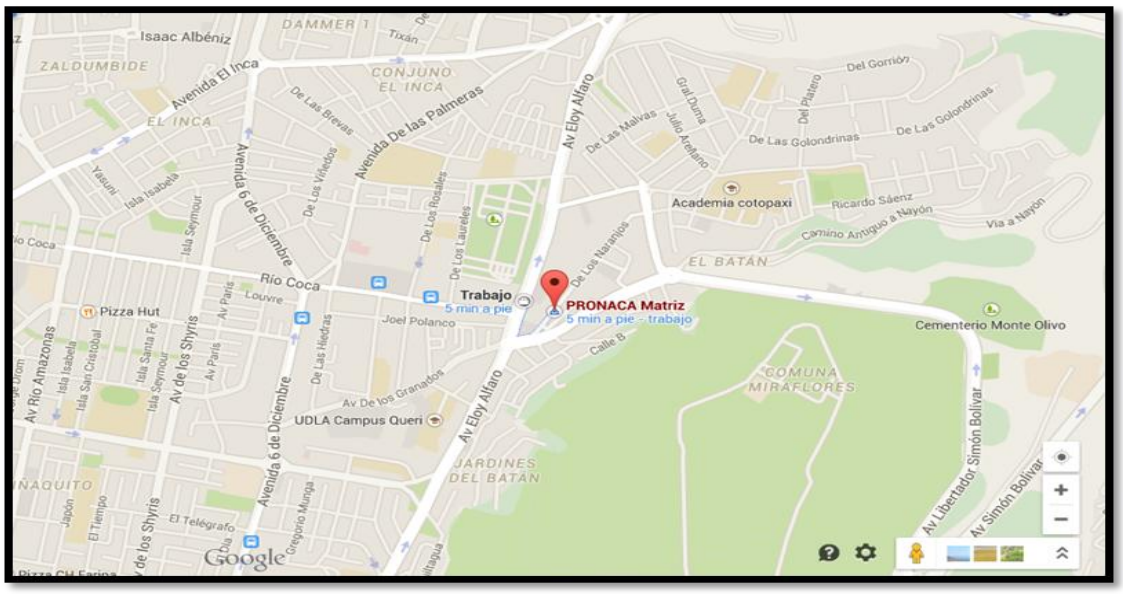


Figura 16: PRONACA Matriz: Av. De Los Naranjos 4415 y Av. Granados

3.4 Zona de Influencia

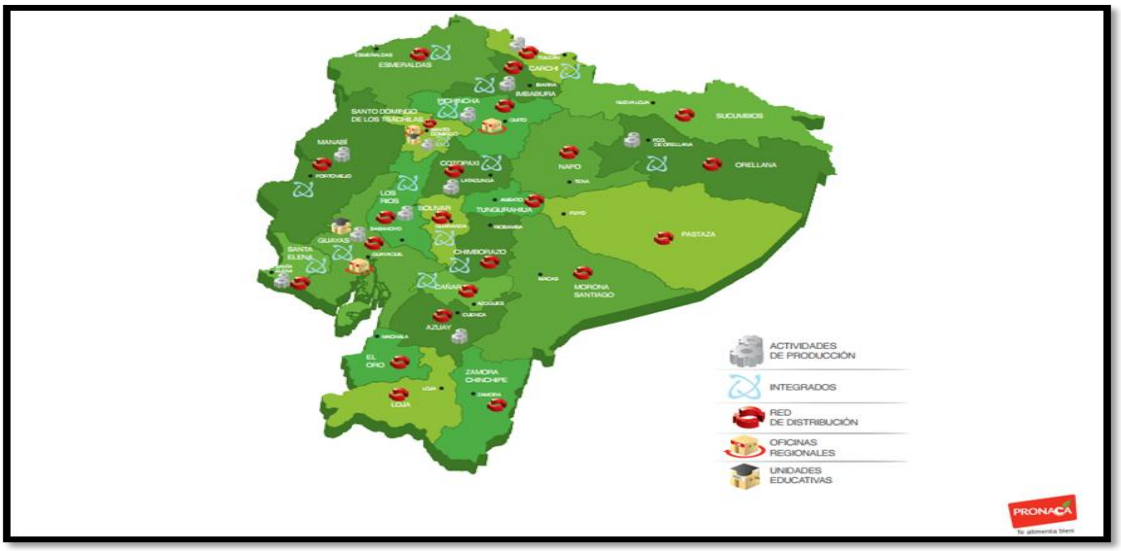


Figura 17: PRONACA en el Ecuador

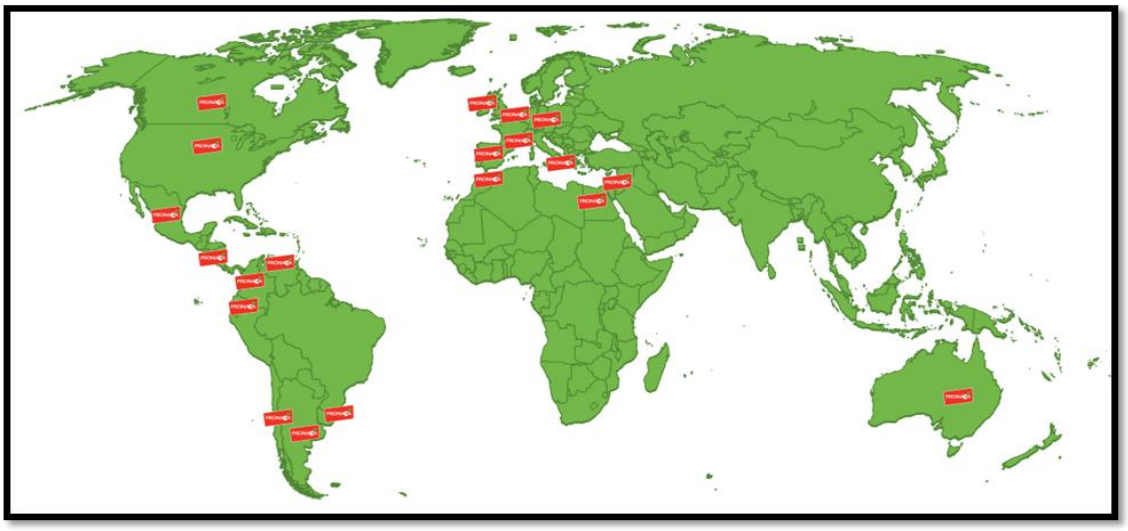


Figura 18: PRONACA en el Mundo

3.5 Misión y Visión

Misión.

La Misión Corporativa de PRONACA juntamente con su razón de ser, establece dedicación del caso a los consumidores y al campo, cada uno de los colaboradores de PRONACA se encuentra prestos para generar desarrollo en el sector agropecuario.

Visión.

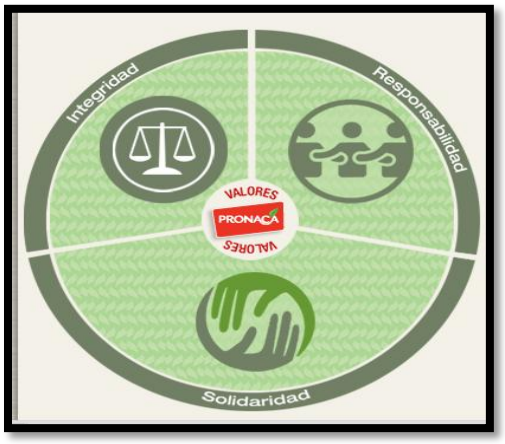
Ser una compañía registrada como ícono de desarrollo y fuente de trabajo. Relacionada como una empresa totalmente ecuatoriana que ofrece calidad.

Filosofía.

PRONACA concurre para alimentar bien generando desarrollo en el sector agropecuario.

Visión.

La cultura de PRONACA está fundamentada en tres valores centrales que inspiran su propósito y los principios que guían sus relaciones.



INTEGRIDAD

En cada uno de sus actos.

RESPONSABILIDAD

Ante los clientes internos y externos.

SOLIDARIDAD

Con sus colaboradores y asociados.

PORTAFOLIO DE SERVICIOS

PRONACA dispone de gran variedad de productos, categorizándolos en cárnicos, embutidos y alimentos para nutrición animal.

Figura 19: Productos de PRONACA

CÁRNICOS

Dentro de los productos cárnicos se dispones:

- **Mr. Pollo,** en todas sus gamas sean enteros, vacíos, en presas, o con vísceras.
- **Mr. Chanco,** en todas sus formas, enteros, en presas o lechón.
- **Mr. Fish,** pescado procesado en filetes.
- **Mr. Cook,** variedad de cárnicos procesados como pre cocidos
- **Mr. Pavo,** en presas y enteros

SECOS

Se categoriza los productos como salsas, enlatados, huevos y arroz que son:

- **Gustadina,** marca para salsas, arroz y mermeladas
- **Rendidor,** arroz pre seleccionado
- **Indaves,** huevos comerciales de diferentes tamaños y costos
- **Rubino,** enlatado, maíz dulce, frutas, entre otras

EMBUTIDOS

En esta categoría se maneja dos tipos de marcas

- Fritz
- Plumrose

NUTRICIÓN ANIMAL

Existe marcas conocidas como:

- **Pro Can,** balanceado para caninos
- **Pro Cat,** balanceado para felinos
- **Pro aves,** balanceado para aves

CARTERA DE CLIENTES

Consumidores

La primera responsabilidad de PRONACA es aprovisionar productos innovadores con características saludables y de alta calidad que alimenten correctamente a sus consumidores y contribuyan al bienestar satisfaciendo a las familias que han depositado su confianza.

Colaboradores

PRONACA lidera a sus participantes con el ejemplo, en forma adecuada, justa y ética profesional. Posee un compromiso solidario y respetuoso con el bienestar de cada uno de ellos y no soporta la deshonestidad.

Promueve el trabajo en equipo y la representación con labor en condiciones no negociables como la seguridad y limpieza.

Ofrece conformidad de oportunidades en los empleos, desarrollo sobre todo la promoción a todos quienes están calificados para ello. Motiva argumentos y acoge sugerencias basadas en recomendaciones de sus colaboradores para el bien de la compañía.

Clientes

PRONACA trabaja junto a sus clientes ofreciendo siempre productos de calidad. Innova sus procesos y productos para liderar los mercados en los cuales está presente. Atiende los pedidos de sus clientes con servicio rápido y prolijo.

Proveedores

Practica el respeto a sus proveedores, a quienes les entrega un beneficio justo en cada negociación, dentro de un marco de comportamiento ético. Siembra el cumplimiento de la ley y una conducta social responsable.

Asociados

Invierte sumas considerables en investigación y desarrollo, crea productos únicos e innovadores. Conlleva altamente su filosofia y crea oportunidades de negocio para sus asociados con quienes salvaguarda una realción cercana y provechosa.

Sociedad

PRONACA opera como un buen ciudadano, siempre busca las mejores relaciones con los incomparables grupos de interes en armonía y colaboración.

Conlleva su experiencia y conocimiento para favorecer al desarrollo y al mejoramiento de la calidad de vida en las áreas de influencia de sus operaciones.

Es respetuosa y solidaria con las personas y con el cuidado minuciioso del equilibrio ambiental.

ESTRUCTURA ORGANIZACIONAL

Para desempeñar las metas y acompañar al crecimiento continuo de PRONACA, la empresa mantiene una estructura organizacional dinámica y que concuerda con los nuevos requerimientos estratégicos planteados.

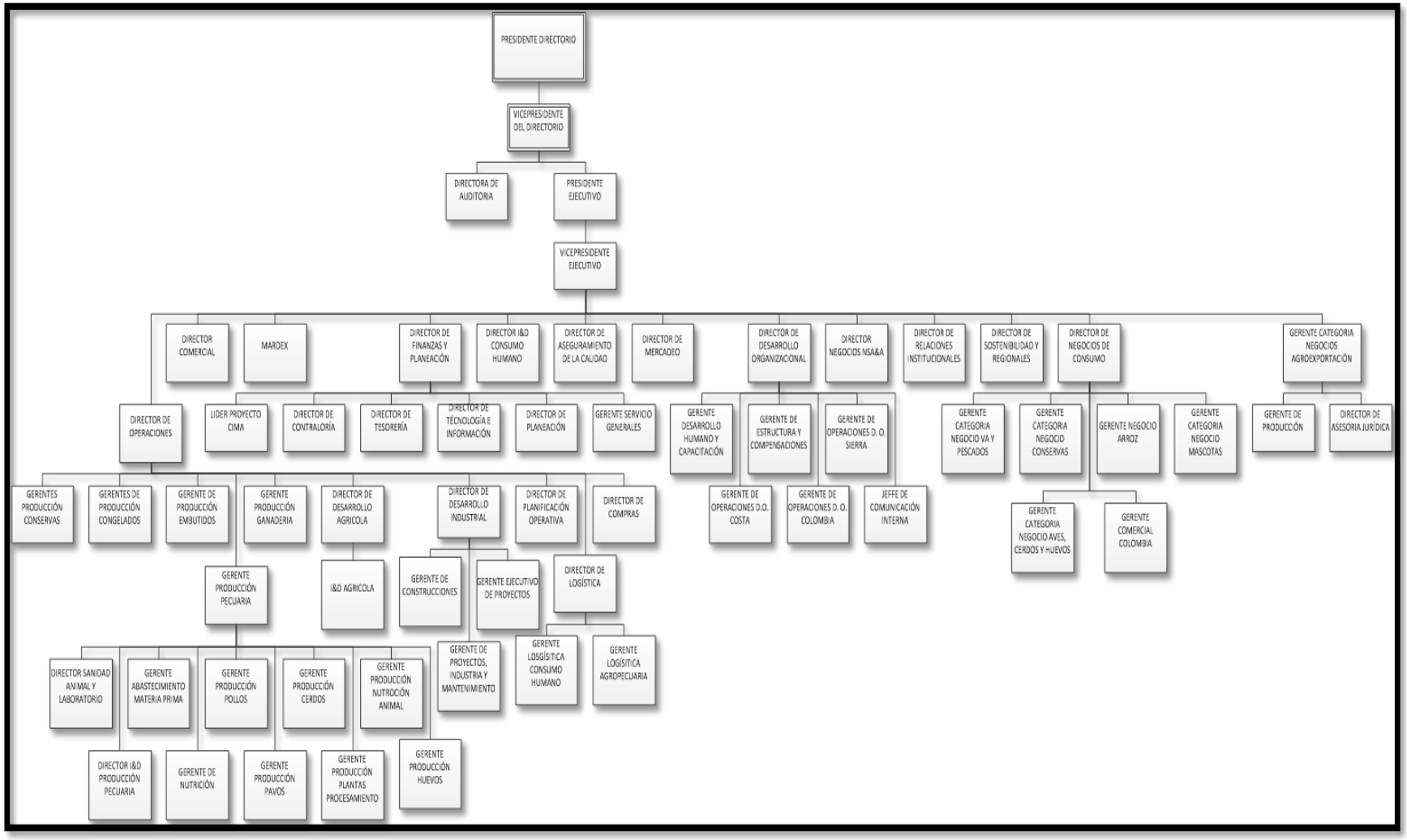


Figura 20: Estructura Organizacional

3.6 Organigrama de TI

En la figura se puede distinguir la estructura actual de TI con la que cuenta PRONACA.

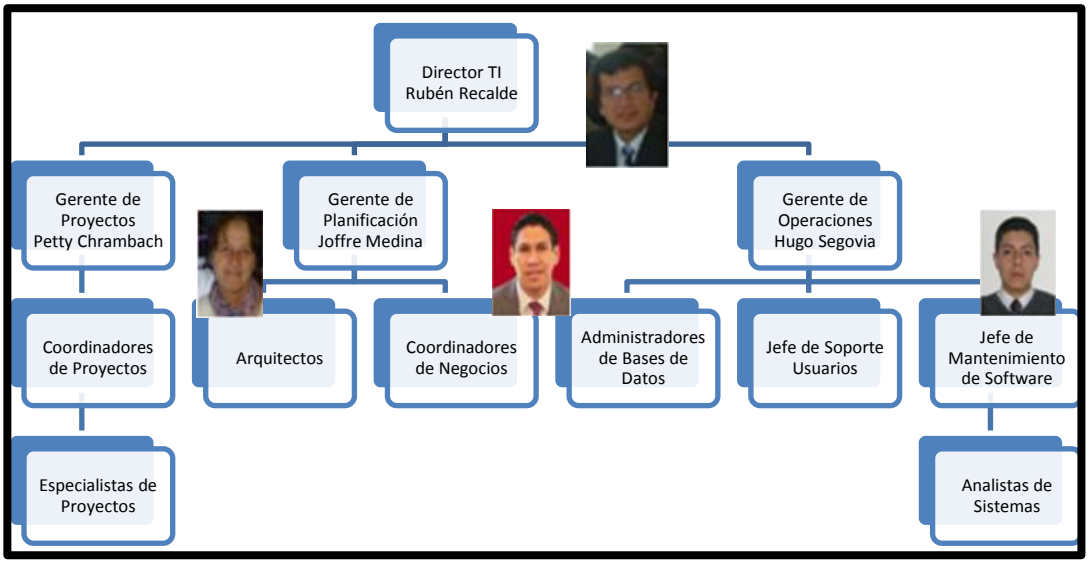


Figura 21: Dirección de TI

3.7 Cadena de Valor de PRONACA.

La figura expresa la cadena de valor bajo la cual PRONACA realiza sus actividades, es muy trascendental aplicar las recomendaciones de las normas ISO 27002 ya que la información posee enunciados primordiales (a-k), se basa en indagación altamente confidencial que es muy segura para evitar cualquier fuga de dicha información.

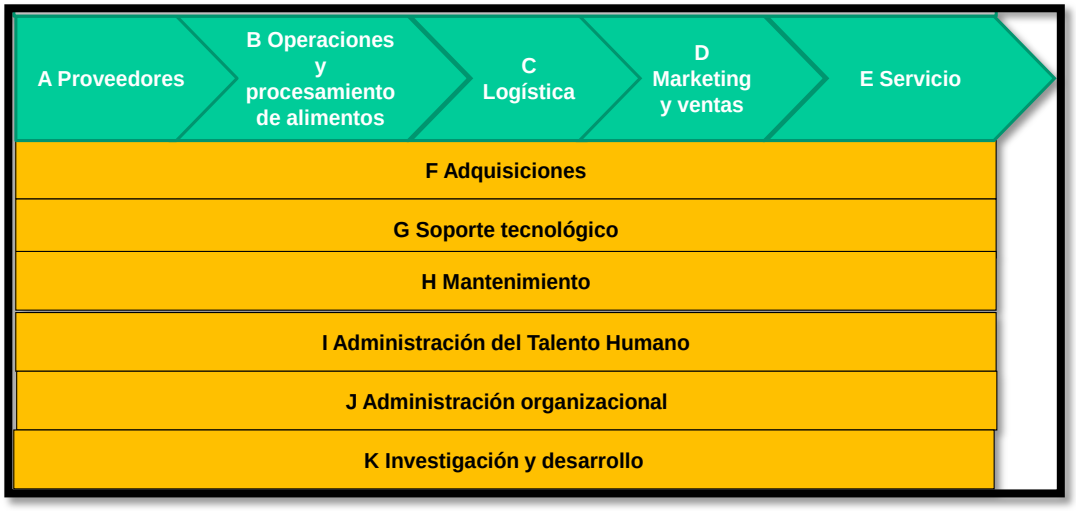


Figura 22: Cadena de Valor

3.8 Análisis de la situación actual de la seguridad informática en Pronaca

Se escogieron dos dominios de la norma ISO 27000, cifrados, seguridad física y ambiental para aplicar en PRONACA ya que son los más ineludibles en este momento, tomando en cuenta los antecedentes de la misma. La norma ISO 27000 sugiere que se puede aplicar las recomendaciones de uno o varios dominios que el usuario elija según la importancia dada.

En la actualidad PRONACA dispone de algunos procedimientos y políticas que no se encuentran basados en la norma ISO27000 pero relativamente se asemejan en ciertos casos, los cuales se encuentran valederos en la intranet de la compañía http://somos:9080/pronaca/homePortalView.htm únicamente para los empleados, dependiendo del área en la que laboren descritos a continuación:

3.8.1 Permisos o privilegios de usuarios.

Por medio de un servidor de Active Directory, se implanta las directrices para los perfiles de Administrador, éstos son proporcionados por técnicos del área de Soporte. Una vez que un usuario tiene creado su perfil, este puede ingresar en cualquier ordenador que se encuentre dentro del dominio de PRONACA.

3.8.2 Password o contraseñas

Al instante de proceder a crear una cuenta, los técnicos de soporte le asignan una clave temporal, la cual debe ser cambiada inmediatamente por el usuario al momento de usar por primera vez la cuenta.

La contraseña nueva y generada debe tener ciertas particularidades para ser validada por ejemplo poseer como mínimo seis caracteres de longitud, no debe ser igual a alguna clave anterior, no debe tener caracteres especiales y al menos una mayúscula.

Si al usuario, por algún motivo se le olvida la contraseña, este deberá solicitar a los técnicos de soporte su respectivo cambio para que el usuario pueda ingresar a su equipo lo más pronto posible.

3.8.3 Inactividad de equipos.

Cuando un usuario, por cualquier motivación deja de utilizar su computador, este se bloqueará en un ciclo de diez minutos, colocándose automáticamente un protector de escritorio indicando la filosofía de PRONACA, una vez transcurrido diez minutos más, el ordenador se pondrá en estado de ahorro de energía, si por alguna circunstancia el usuario necesita que su computador no se ponga en curso de ahorro de energía, este debe mostrar la debida justificación al administrador de red para que proceda a quitarle dicha política de bloqueo.

PRONACA al ser una empresa que se alinea objetivamente a las Políticas de Estado, obligatoriamente dispone de software con licencias originales, de lo cual, como política institucional ningún usuario puede instalar alguna aplicación.

3.8.4 Uso de internet

Objetivo

Definir notoriamente, lineamientos generales para asegurar una adecuada protección de la información en el uso de los servicios a Internet.

Alcance

Esta táctica es aplicable a PRONACA y a todas sus compañías relacionadas, para que los usuarios puedan acceder a internet de manera segura, únicamente a páginas previamente autorizadas.

Exposición del procedimiento

Sin excepción alguna, todas las conexiones deben realizarse a través de un firewall. En el caso muy particular de las conexiones satelitales, deben

ser validadas a través de un servidor de tipo AAA para comprobación de autenticidad, a fin de inspeccionar los accesos de los usuarios, para lo cual se debe llevar una bitácora de registro de todos los servicios utilizados.

Para el acceso al Internet es inevitable obtener la autorización por parte del Gerente del negocio o Director corporativo correspondiente, quien colaborará e impartirá la configuración del servicio que debe utilizarse para tareas propias de la función desarrollada en la compañía

Responsabilidades

Aplica absolutamente para todos los empleados y usuarios inmersos de PRONACA y todas sus compañías relacionadas donde se acota las directrices estipuladas por Director Corporativo de Tecnología y Medios

3.8.5 Acceso al Data Center

Objetivo

Instituir políticas generales para la definición y estricto control de los registros de acceso al Data Center en la oficina matriz.

Alcance

Aplicable únicamente al personal de Tecnologías de la Información que tienen acceso al Data Center y al personal de la Cabina de Seguridad del Edificio Inverna.

Exposición del procedimiento

El sistema de control de acceso humano que se encuentra instalado en las puertas del Data Center tiene su programación y generación de reportes a través de la consola que administra el personal de la Cabina de seguridad donde se puede obtener un reporte cuando sea necesario.

El Gerente Técnico es la única persona que autoriza el ingreso al Data Center, a través de una programación que realiza el personal de la Cabina

de Seguridad con las tarjetas de acceso, sean estos Administradores de Base de Datos, Arquitecto de Aplicaciones o Analistas de Sistemas.

Responsabilidades

- Gerente Técnico y Telecomunicaciones
- Área de seguridad física.
- Arquitectos de Aplicaciones, Administradores de Base de Datos, Analistas de Sistemas.

3.8.6 Administración y control de acceso a la Información

Objetivo

Delimitar el proceso que afirme a todos los usuarios para la obtención en el acceso a la información para el desarrollo de sus tareas habituales en la compañía y fiel cumplimiento de las mismas.

Alcance

Aplicable para todos los sistemas que son de uso concurrente en PRONACA y de sus compañías Relacionadas, siempre y cuando la tecnología lo permita.

Exposición del procedimiento

Instauración de un usuario cuando un colaborador requiere acceso a un sistema informático, se le puede modificar mediante los accesos cuando estos sean demandados. Los usuarios solo deben tener permisos de acceso a los recursos para los cuales estén debidamente autorizados y que hayan sido otorgados por su necesidad de trabajo y giro de negocio.

Para gobernar los accesos de los usuarios, se debe cumplir con los siguientes requisitos como la solicitud de accesos por parte de nómina en talento humano, autorización que depende de las tareas habituales que desarrollara el usuario y al mismo tiempo la autenticación asignada por medio de una clave

Responsabilidades

- Consejo de Directorio
- Colaboradores y usuarios
- Gerentes de Negocio y Directores Administrativos
- Dirección de Desarrollo Organizacional e Institucional
- Director de Tecnología y Medios
- Dirección de Auditoría y Contraloría.

3.8.7 Adquisición de bienes y servicios de Tecnología.

Objetivo

Implantar lineamientos claros para adquirir productos o servicios de Tecnología en la Información.

Alcance

Política aplicable a PRONACA y sus compañías relacionadas a nivel nacional.

Exposición del procedimiento

El personal de soporte a usuarios de TI recibirá los requerimientos de hardware y software por parte de los usuarios normales administrativos, donde se validará el requerimiento y se lo enviará a la Gerencia de Soporte de Usuarios para el trámite respectivo.

Las compras de activos fijos como computadoras, servidores, switches, centrales telefónicas, teléfonos, proyectores, impresoras, entre otors deben ser canalizados a través de la Gerencia Técnica enviando el requerimiento vía mail, inmediatamente se llena un formulario interno provisto por el área que a su paso será aprobada por la Dirección de Tecnología para posteriormente comprar a través del departamento de compras del edificio matriz.

Si consta o hallases daño en un equipo que no puede ser reparado por el personal de Soporte a Usuarios, este deberá ser enviado a un servicio

técnico autorizado que previamente haya sido calificado con los estándares de la compañía como proveedores.

Al instante de calificar a una empresa o distribuidor como proveedor se toma en cuenta los siguientes aspectos: financiero, calidad, logística, responsabilidad comprobada y servicio de garantía total.

Responsabilidades

- Dirección de compras
- Dirección de Tecnología Informática

3.8.8 Adquisición de nuevos proyectos de tecnología.

Objetivo

Crear las etapas a seguir para el desarrollo o adquisición de una aplicación de un Software que la compañía demanda para automatizar un proceso.

Alcance

Aplicable al área de Proyectos de Tecnología de PRONACA y sus compañías Relacionadas.

Exposición del procedimiento

Objetivos que son planteados para posteriormente definir la situación actual y la representación del nuevo requerimiento. La revisión de la planificación y ejecución del proyecto se inspeccionará si el proyecto no está planificado mucho menos presupuestado, de la misma manera si no constase en el plan de trabajo del año en curso, el área de Tecnología tendrá la obligación directa de revisar la disponibilidad de los recursos juntamente con los costos del proyecto el área solicitante.

Cuando se proceda a dar luz verde con la aprobación, se pasa a la definición de la herramienta y recursos del proyecto, donde se reunirá el

Gerente Técnico, Coordinador de sistemas del área, Gerente de Proyectos para su revisión, y análisis de los requerimientos para ser ejecutados. El nuevo Software se lo puede adquirir de varias maneras, como son:

- **Desarrollo interno**. Con recursos netamente propios de la organización.
- **Desarrollo externo**. Puede ser tercerizado según la aplicación que se requiera donde la arquitectura del hardware y la herramienta en la que se desarrollará serán responsabilidades del proveedor de Software, el mismo que debe estar completamente calificado como socio de negocios del grupo.
- **Software comprado**. Puede ser un sistema comprado, es decir desarrollado a medida con su respectivo lenguaje y arquitectura.

Para el desarrollo y perfeccionamiento del proyecto, se conforma un grupo interno de especialistas que estará a cargo durante el paso a paso de todo el desarrollo hasta su finalización.

Responsabilidades

- Carpeta del proyecto, que estará bajo la responsabilidad del Analista Programador interno de la organización.
- Carpeta control de Hitos de Proyecto, que estará bajo la responsabilidad del Gerente de Proyectos de TI.
- Carpeta de Aplicaciones Data Center, que estará a cargo del Gerente de Proyectos de TI.

3.8.9 Evaluación y riesgo tecnológico

Objetivo

Definir las pautas generales para identificar y evaluar los conflictos debido al uso tecnológico con sus respectivas herramientas, adicionalmente como parte del proceso global de manejo de todos los riesgos en PRONACA se debe tomar medidas precautelatorias.

Alcance

Este procedimiento es aplicable a PRONACA y sus compañías Relacionadas, con el objetivo de llegar a obtener una evaluación del riesgo tecnológico, que permita minimizar al máximo los posibles riesgos de seguridad.

Exposición del procedimiento

La estimación del riesgo tecnológico está dirigida hacia los recursos de información muy relevantes para el giro de negocio, es decir, todos los recursos tecnológicos son de apoyo para la organización en PRONACA para alcanzar sus metas planteadas.

Los técnicos convendrán identificar los riesgos sobre los recursos y evaluar el posible impacto en los negocios si alguno de los riesgos se materializa, al mismo tiempo los técnicos serán los agentes de evaluar la flaqueza hacia los riesgos, tomando en consideración las medidas de seguridad existentes a fin de implantar la probabilidad de que el riesgo se convierta en un evento real.

Responsabilidades

- Comité de Seguridad de la Información
- Director corporativo de Tecnología y Medios
- Gerencias de Negocio y Direcciones Corporativas

3.8.10 Seguridad de incidentes del personal.

Objetivo

Minimizar el riesgo de errores de carácter humano al igual que las amenazas o mal uso de los Sistemas de información relevantes para PRONACA, de igual cerciorar que los empleados tomen conciencia de las amenazas que existen sobre seguridad de la información.

Alcance

Este procedimiento es aplicable a todo el personal, no se permitirán excepciones excepto bajo aprobación del Presidente del Comité de

Seguridad de la Información, quién custodiará a documentación de soporte durante el tiempo necesario.

Exposición del procedimiento

Los trabajos de seguridad están incluidas en la gestión de PRONACA desde el ciclo de reclutamiento del personal, etapa de contratación y concluyendo con el seguimiento de la desvinculación laboral.

Imperiosamente, para trabajos de alta sensibilidad los alistamientos potenciales del personal deben ser monitoreados en este aspecto. Todos los empleados firmarán un acuerdo de confidencialidad.

La seguridad de la información es un segmento integral del proceso de negocios y aflige a cada empleado que usa la tecnología de información en su trabajo. Todos los empleados con dirección a los sistemas de información de PRONACA firmarán un acuerdo de confidencialidad, como parte de las condiciones y políticas de empleo.

Se requiere una preparación apropiado hacia los colaboradores el cual debe ser estipulado como mínimo una vez al año, sin dejar a lado las actualizaciones periódicas sobre las regulaciones de seguridad de la información.

Los procedimientos sobre acontecimientos cubren todo tipo de incidentes de seguridad de la información potenciales, como fallos divisados en la seguridad y pérdida de servicios. Todos los empleados deben reportar cualquier incidente de seguridad a través de la comunicación directa a la Gerencia. Los usuarios no deben por si mismos tratar de eliminar cualquier infracción sospechosa, debiendo considerar las pruebas de contingencia a ser realizadas por mal uso del sistema.

Toda divulgación no autorizada de información se considerará como falta grave y se aplicará las sanciones respectivas del caso según el reglamento

interno de PRONACA. Para otro tipo de incumplimientos su gravedad será calculada por el Comité de Seguridad de la Información a fin de designar la sanción correspondiente.

Responsabilidades

- Empleados y usuarios
- Gerente de Negocio y Directores Corporativos
- Director Corporativo de Desarrollo Organizacional

Una vez definidas las políticas e instrucciones actuales en las que se basa PRONACA, es imperioso realizar una reclasificación y en algunos casos la reutilización de políticas que hacen referencia a las recomendadas por la norma ISO 27002.

CAPÍTULO IV

IMPLEMENTACIÓN DE DOS DOMINIOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA PRONACA.

Generalidades

PRONACA cuenta con investigación muy relevante, por lo cual en el período de protección de sus datos no se puede escatimar ningún tipo de recurso.

Es ineludible la creación de Políticas de Seguridad de la Información que minimicen los riesgos a los cuales se enfrenta la organización, organizando en primer lugar una cultura organizacional que envuelva a los empleados y accionistas de la empresa.

En PRONACA los reglamentos son determinados y muy claros en su alcance para así poder verificar su cumplimiento y ejecución. Consecuentemente cualquier política a definir mantendrá el mismo formato.

Objetivo

Proteger ante cualquier amenaza de índole interna o externa la Información de la compañía, mediante el uso de las Políticas de Seguridad de la Información, recomendadas por los esquemas Internacionales de la ISO27001 e ISO27002.

Alcance

Las políticas recomendadas en este manual, se aplican a el área de Tecnología de la Empresa en los ámbitos de los dos dominios expuestos: Cifrado y Seguridad Física y Ambiental, con sus respectivos objetivos y controles.

Este manual tiene como finalidad proporcionar directrices, procedimientos y requisitos, que puedan a futuro ser implementados organizacionalmente.

Mapa conceptual de los dominios a usar

En la figura 23, se puede observar un mapa claro y conceptual de los dos dominios con sus respectivos objetivos, que son esencia de la implementación para PRONACA.

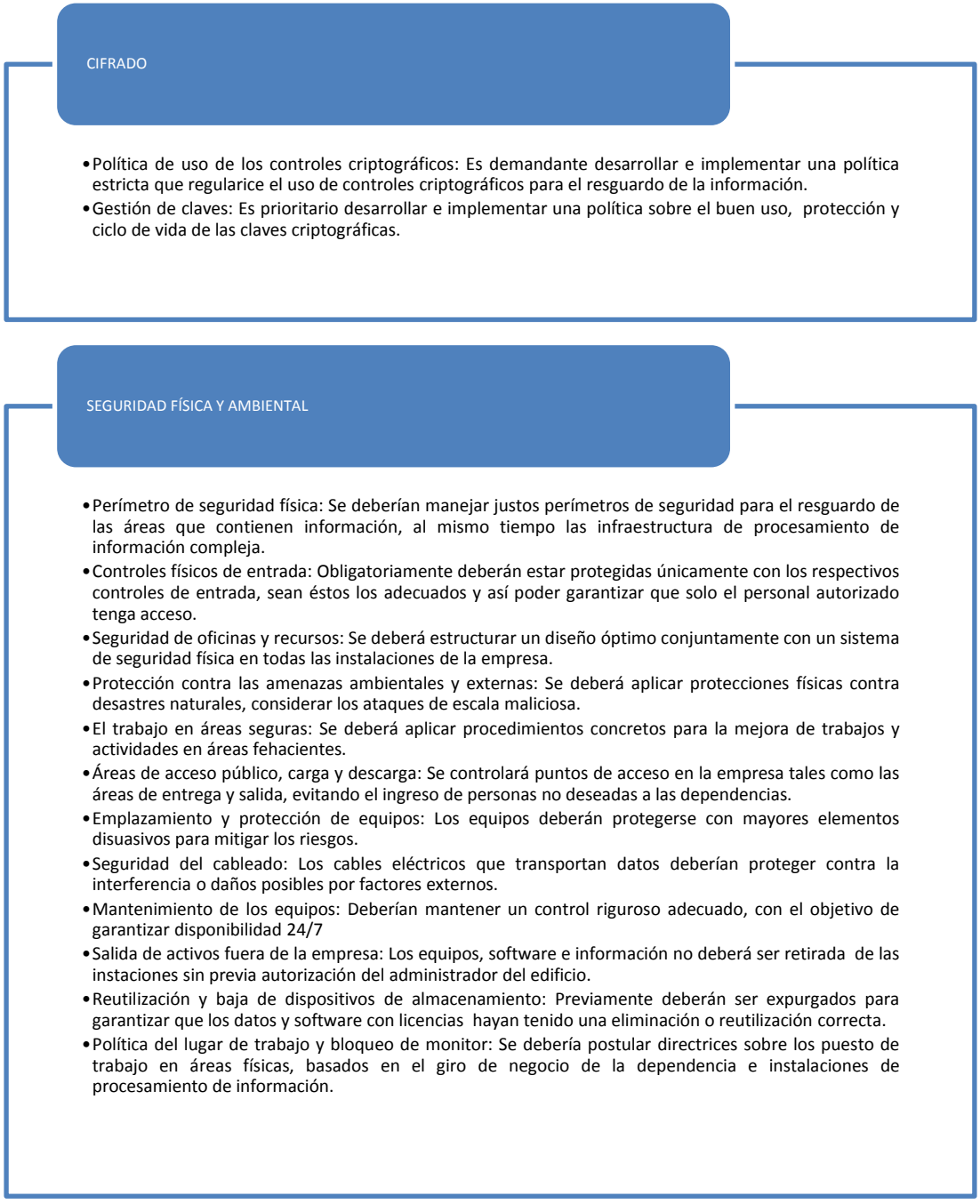


Figura 23: Mapa conceptual de los 2 dominios de la norma ISO 27002. (ISO2700.ES, 2012)

4.1 Cifrado

4.1.1 Controles Criptográficos

Objetivo:

Proteger la confidencialidad, autenticidad e integridad de la información referente a la prestación de servicios a través de medios criptográficos.

- **Política sobre el uso de controles criptográficos**

a) Quien se encargue de formalizar y administrar los controles criptográficos será el Área de Seguridad de la Información.
b) Para atestiguar la correcta actividad antes de la implementación en modo producción se deberá obligatoriamente hacer pruebas de controles de encriptación en un ambiente de ensayos. El Director de TI será quien consienta su paso a producción.
c) Debido a la jerarquía de atención prioritaria, no se debe aplicar ningún tipo de controles de encriptación en los casos como el monitoreo de virus e interfaces.
d) Se debe avalar que el uso de los medios criptográficos no afecte la entrega de la información.
e) Con la mira de evitar cualquier novedad en la información de los cheques de pagos a proveedores en el Área de Tesorería se debe utilizar controles criptográficos.

- **Gestión de claves**

a) Dentro de la compañía, el responsable directo de generar claves encriptadas para las aplicaciones y sistemas será el Área de Seguridad de la Información.
b) Se debe generar un documento de aceptación de condiciones basadas en la confidencialidad y privacidad entre el Área de Seguridad de la Información y la parte solicitante, con firmas de responsabilidad.
c) Con el único objetivo de obtener una exploración de los tiempos en los cambio de claves y de posibles incidentes producidos, se deberá

mantener un archivo histórico incluyendo perfectamente las claves actuales y antiguas.

d) Se verificará constantemente que no se encuentre utilizando en ninguna interfaz una clave previa a su modificación o inactivación.
e) Deben ser defendidas contra difusión no autorizada y cualquier tipo de daño, transformación y pérdida las claves criptográficas de la empresa.
f) Por motivo de legitimación, cada clave deberá ser usada de forma correcta y sin riesgo para la empresa, cada seis meses se debe realizar un escrutinio interno de la gestión de claves.
g) En caso de presentarse una salida de empleado o un incidente de descubrimiento de clave, se procederá con el cambio inmediato por el Área de Seguridad de la Información.
h) Se debe precisar un periodo de tres meses para el funcionamiento de una clave, transcurrido este tiempo debe cambiarse. El Área de Seguridad de la información es garante de asignar esta vigencia.

4.2 Seguridad física y ambiental

4.2.1 Áreas Seguras

Objetivo

Evitar el acceso físico no autorizado, daño e interferencia con la información y locales de la empresa. Se deben definir áreas seguras donde se puedan proteger los medios de procesamiento y almacenamiento de información de PRONACA con perfectos e inviolables controles de entrada apropiados.

- **Perímetro de seguridad física**

a) Es necesaria un área de recepción con medios de identificación y control de acceso físico, únicamente el personal autorizado podrá tener acceso
b) El edificio no debe tener brechas para evitar el ingreso no autorizado.

Todos los ingresos deben ser debidamente protegidos con vallas, puertas, alarmas, entre otros. Y mantenerse aseguradas mientras no sean utilizadas.

c) Dependiendo de los activos y evaluación del riesgo se debe definir claramente los perímetros de seguridad a la redonda.
d) Se debe contar con monitoreo constante, es decir las veinte y cuatro horas en todas las puertas de emergencia en el perímetro de seguridad.
e) Se debe poseer sistemas de detección de intrusos acordes con estándares internacionales, regionales y nacionales, y deben ser probadas periódicamente su eficacia.

- **Controles de ingreso físico**

a) Se debe controlar y restringir mediante controles de autenticación solo a personas autorizadas el acceso a áreas donde se procesa o almacena información sensible.
b) Se debe otorgar acceso restringido a las áreas seguras de información solo cuando sea necesario al personal de servicio de apoyo.
c) Sin lugar a duda. todos los empleados y visitantes deberán poseer una credencial visible todo el tiempo.
d) Los derechos de acceso a áreas seguras serán revisados y actualizados regularmente, de ser el caso revocados cuando sea necesario.

- **Protección contra amenazas externas e internas**

a) El equipo contra incendios debe cumplir los estándares manejados como empresas de alta sensibilidad
b) La papelería y suministros deben almacenarse y protegerse en un área asegurada anti incendios.
c) Los materiales catalogados como peligrosos, deben estar a una distancia estrictamente segura.
d) Para evitar posibles daños, los equipos de reemplazo y los medios de respaldo deben ubicarse fuera de las instalaciones del edificio principal

- **Trabajo en áreas aseguradas**

a) El trabajo en el área asegurada siempre debe ser monitoreado.
b) Sin la respectiva autorización, no se debe permitir fotografías ni grabaciones
c) Todo tipo de actividad, incluyendo arreglos y mantenimientos dentro del área asegurada deberán ser registradas y verificadas conjuntamente con documentos de controles

- **Áreas de acceso público, entrega y carga**

a) Se debe registrar el material tanto de ingresa como de salida para evitar amenazas potenciales.
b) Se debe delimitar el área de recepción tras la puerta de ingreso controlada, para que desde esta se direccione específicamente al personal en base a las necesidades de cada caso.

4.2.2 Equipo de seguridad

Objetivo

Evitar radicalmente la pérdida, daño o hurto de los activos e interrupción de las actividades de la organización.

- **Ubicación y protección del equipo**

a) Los ítems que necesitan protección especial deben ser aislados para reducir el nivel general de la protección requerida.
b) Se debe monitorear continuamente las condiciones ambientales con el fin de prevenir posibles afectaciones.
c) Se debe implementar controles de detección y respuestas a potenciales amenazas como la falla en el suministro de agua, humo, vibración, entre otras e interferencias en el suministro eléctrico.
d) En el perímetro próximo a los medios de procesamiento de información se debe evitar completamente el ingerir alimentos o bebidas que al mismo tiempo darán prioridad al no permitir el cigarrillo.

e) Para reducir el riesgo donde la información sea vista por personas no autorizadas, se debe manera procesos de resguardo para evitar el acceso no autorizado.

- **Servicios públicos de soporte**

a) Todos los servicios públicos de soporte; como telefonía, internet, electricidad, desagüe y suministro de agua; deben adecuarse a los sistemas que soportan.
b) Con el fin de reducir cualquier riesgo por un mal funcionamiento o falla, se debe inspeccionar, probar y monitorear continuamente los servicios públicos de soporte
c) Es recomendable proveerse de un dispositivo de suministro de energía ininterrumpido (UPS) y generadores de energía, que sirvan como plan de contingencia para la energía, tomando en cuenta que la falla de energía podría ser prolongada.
d) Con el fin de asegurar el uso prolongado del generador, se debe tener disponible suficiente suministro de combustible.
e) Para prevenir cualquier emergencia que se relacione con el servicio de energía se deben colocar en las habitaciones donde se encuentra el equipo, interruptores de emergencia.
f) Debe existir iluminación de emergencia para prevenir una falla en la fuente de energía principal.
g) Debe instalarse un sistema de alarma para detectar mal funcionamiento en los servicios públicos de soporte.
h) Para evitar que una falla en la conexión afecte el desempeño de los servicios de voz, los equipos de telecomunicaciones deben conectarse por lo menos en dos rutas al proveedor del servicio.
i) Los servicios de voz debieran ser adecuados para cumplir con los requerimientos legales de las comunicaciones de emergencia.

- **Seguridad del cableado**

a) Se debe proteger adecuados el cableado de la red, para así evitar intercepciones no autorizadas o daños.

b) De ser posible deben ser subterráneas o estar sujetas a una alternativa de protección adecuada
c) Se deben identificar debidamente, utilizado etiquetas y marcadores de cables las líneas de energía y telecomunicaciones
d) Con el objeto de evitar interferencia los cables de comunicaciones debes estar separados de los de energía.
e) Se deben considerar controles especiales para sistemas más sensibles, tales como:
    1) Iniciación de barridos técnicos e inspecciones físicas de dispositivos
    2) Instalación de un tubo blindado y espacios con llave en los puntos de inspección.
    3) Utilización de rutas alternativas ante los medios de transmisión de seguridad adecuada
    4) Uso de cableado con fibra óptica y manipulación por expertos certificados

- **Mantenimiento de equipos generales**

a) Las reparaciones y servicios de mantenimiento deben ser realizadas únicamente por el personal autorizado.
b) Deben cumplirse todos los requerimientos definidos por las pólizas de seguros.
c) Debe llevarse correctamente una bitácora de registro donde se describa todas las fallas sospechadas y reales.

- **Seguridad del equipo fuera de la empresa**

a) Debe estar a la mira que se cumpla a cabalidad y en todo momento las instrucciones de los fabricantes para protección de los equipos.
b) Si un equipo sale de las instalaciones de la empresa, éstos deben ser protegidos con un fehaciente contingente.
c) En caso de realizarse trabajo en casa, se debe implementar controles apropiados

- **Seguridad en la eliminación o reutilización de equipos**

a) Revisar los archivos que posee cada equipo para asegurar que se elimine cualquier elemento confidencial
b) Demandantemente se debe destruir físicamente todo equipo que posea información confidencial.
c) Dependiendo del resultado evaluación de riesgo se debe determinar si los dispositivos debieran ser físicamente destruidos

- **Retiro de propiedad o suministro tecnológico**

a) Debe inspeccionarse el retiro del suministro con actas de recepción, donde se identificará a detalle un desglose del bien
b) Claramente debe identificarse que todo personal tenga la potestad para permitir el retiro de los activos fuera de la empresa.

CAPITULO V
CONCLUSIONES Y RECOMENDACIONES.

5.1 Conclusiones.

- Se tomó en cuenta como punto inicial las normas y políticas vigentes en PRONACA para en base a estas proponer el SGSI presentado.
- Se siguió las normas internacionales ISO 27001 e ISO 27002 en la realización de este trabajo, debido a que la información se ha convertido en PRONACA como a nivel mundial en el activo más valioso empresarialmente, por lo tanto, es fundamental realizar una correcta gestión de la misma a fin de que se encuentre segura, confiable y disponible permanentemente.
- Con el fin de minimizar al máximo, los riesgos que se puedan presentar en la seguridad de la información de PRONACA, se inició determinando la situación actual de la compañía para culminar con el diseño de un Sistema de Gestión de Seguridad de la Información, con los dominios de Cifrado y Seguridad Física y Ambiental de la norma ISO 27002.
- Con las recomendaciones de los estándares internacionales ISO 27001 e ISO 27002 aplicadas en la propuesta expuesta será posible mantener segura, disponible y confiable la información de PRONACA, obteniendo altos niveles de seguridad.
- Habiéndose definido recientemente en PRONACA un Área de Seguridad de la Información es imprescindible que esta defina cada uno de los recursos tecnológicos con los que cuenta la compañía y se haga responsable de evitar riesgos que pueden afectar la correcta operatividad de los procesos de la organización.

5.2 Recomendaciones.

- Es mejor ser proactivo y prevenir violaciones a la seguridad, evitando riesgos y amenazas innecesarias que podrían generar problemas para la organización, que tener luego que realizar acciones correctivas.
- Es aconsejable realizar análisis a las políticas expuestas periódicamente ya que día a día van surgiendo nuevas amenazas que podrían afectar la seguridad de la compañía.
- Se recomienda que el área de Seguridad de la Información realice, constantes monitoreos y actualizaciones de cada tarea e incidencias presentadas, así como de las políticas de seguridad de la empresa. Como también es necesario que el personal de esta área se encuentre en constante capacitación sobre Sistemas de Gestión de Seguridad de la Información.
- Es necesario llevar un registro de las incidencias y sus respectivas acciones correctivas realizadas. Además de tener documentado un procedimiento operativo donde se detallen los mantenimientos programados.
- El área de Seguridad de la Información debe ser responsable de publicar, concientizar y motivar a las demás áreas de la empresa, para que cada uno se haga responsable por cumplir a cabalidad las políticas y recomendaciones instituidas, precautelando así el buen estado de la información.
- Para evitar generar incompatibilidades y vulnerabilidades no previstas en las aplicaciones manejadas por la compañía, se recomienda siempre realizar varias pruebas de funcionalidad antes de implementar cualquier control de la norma.

REFERENCIAS BIBLIOGRÁFICAS Y ELECTRÓNICAS

Baldeón, M. &. (2012). *PLAN MAESTRO DE SEGURIDAD INFORMÁTICA PARA LA UTIC DE LA ESPE CON LINEMIENTOS DE LA NORMA ISO/IEC 27002.* Sangolquí: ESPE.

Erb, M. (1999). *Gestión de Riesgo en la Seguridad Informática*. Obtenido de https://protejete.wordpress.com/gdr_principal/reduccion_riesgo/

Flores, F. &. (2010). *DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA MEGADATOS S.A. EN LA CIUDAD DE QUITO, APLICACANDO LAS NORMAS ISO 27001 E ISO 27002.* Quito: EPN.

Guerrero, R. (2009). *DESARROLLO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA E IMPLEMENTACIÓN DE TRES DOMINIOS EN BASE A LA NORMA 27002 PARA EL ÁREA DE HARDWARE EN LA EMPRESA UNIPLEX SYSTEMS S.A. EN QUITO.* Quito: EPN.

INCONTEC. (2008). *Norma Técnica Colombiana NTC-ISI/IEC 27005.* Bogotá: INCONTEC.

INDECOPI. (2012). *NTP-ISO/IEC 27003 Directrices para la implementación de un SGSI.* Lima: 1ra Edición.

ISO/IEC. (2009). *Descripción general y vocabulario.* Suiza.

ISO/IEC. (2009). *Técnicas de la seguridad.* Suiza: ISO/IEC 2009.

ISO2700.ES. (2012). *El portal de ISO 27001 en español*. Obtenido de http://www.iso27000.es/iso27000.html

ISO27000.es. (2005). *El portal de ISO 27001 en español*. Recuperado el 31 de 08 de 2013, de http://www.iso27000.es/iso27000.html#section3a

ISO27002, I. 1. (2005). *Código para la práctica de la gestión de la seguridad de la información.* Bogotá.

Jaimes, A. J. (02 de 06 de 2009). *Gerencia de Tecnología de Información*. Obtenido de http://inf-tek.blogia.com/2009/060203-8.3-amenazas-y-vulnerabilidades.php

MENDOZA, M. Á. (29 de 09 de 2014). *welivesecurity*. Obtenido de http://www.welivesecurity.com/la-es/2014/09/29/8-pasos-evaluacion-de-riesgos-1/

Neira, A. L. (2012). *ISO2700*. Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf

Pressman, R. S. (2002). *Ingeniería del Software.* Madrid: McGRAWN-HILL.

PRONACA. (2010). *Procedimientos Internos.* Quito.

Rhand Leal, A. J. (2012). *270007 Academy*. Obtenido de http://advisera.com/27001academy/es/que-es-iso-27001/

Roldán, C. S. (07 de 09 de 2012). *Codejobs*. Obtenido de https://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo

SGS, E. (2013). *Auditor interno ISO 27001:2005.* Quito: SGS.

UNIT, I. U. (2005). *Normas UNIT-ISO/IEC 27000.* Montevideo: UNIT.

Universidad de Colombia. (2012). *Método de Control de Proceso*. Obtenido de http://www.unalmed.edu.co/josemaya/Ing_prod/Control%20de%20Proceso-%20Metodo.pdf