VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

UNIDAD DE GESTIÓN DE POSTGRADOS

TESIS DE GRADO MAESTRÍA EN GERENCIA DE REDES Y TELECOMUNICACIONES
II PROMOCIÓN

TEMA: “DISEÑO PARA LA IMPLEMENTACIÓN DE TRES DOMINIOS DE UN SISTEMA DE GESTIÓN EN LA SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO27001 E ISO27002, PARA EL ÁREA DE SOFTWARE DE LA PROCESADORA NACIONAL DE ALIMENTOS PRONACA”.

AUTOR: MORALES, RODOLFO FABIÁN

DIRECTOR: ING. ALTAMIRANO, DANIEL

SANGOLQUI, ENERO 2015

i

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

CERTIFICADO

Que el trabajo titulado "DISEÑO PARA LA IMPLEMENTACIÓN DE TRES DOMINIOS DE UN SISTEMA DE GESTIÓN EN LA SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO27001 E ISO27002, PARA EL ÁREA DE SOFTWARE DE LA PROCESADORA NACIONAL DE ALIMENTOS PRONACA", y el documento científico en su totalidad, han sido realizados por el Ing. Rodolfo Fabián Morales Arévalo, ha sido guiado y revisado periódicamente y cumple con las normas estatuarias establecidas por la ESPE, en el reglamento de estudiantes de la Universidad de las fuerzas Armadas.

El mencionado trabajo consta de un documento empastado, un disco compacto, el que contiene los archivos del formato digital.

Autorizan al Ing. Rodolfo Fabián Morales Arévalo que lo entregue al Ing, Paúl Ayala Msc. en calidad de coordinador de la Maestría en Gerencia de Redes y Telecomunicaciones.

Sangolquí, 23 de enero 2015

Ing. Daniel Altamirano Msc.
DIRETOR

ii

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

DECLARACIÓN DE RESPONSABILIDAD

Yo, Rodolfo Fabián Morales Arévalo, declaro bajo juramento que el trabajo aquí escrito es de mi autoría; que no ha sido presentado previamente para ningún grado o calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaro que cedo mi derecho de propiedad intelectual correspondiente a este trabajo a la Universidad de las Fuerzas Armadas-ESPE, según lo establecido por la ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

Ing. Rodolfo Fabián Morales A.

iii

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

AUTORIZACIÓN

Yo, Rodolfo Fabián Morales Arévalo

Autorizo a la Universidad de las Fuerzas Armadas-ESPE la publicación en la biblioteca virtual de la institución el trabajo "DISEÑO PARA LA IMPLEMENTACIÓN DE TRES DOMINIOS DE UN SISTEMA DE GESTIÓN EN LA SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO27001 E ISO27002, PARA EL ÁREA DE SOFTWARE DE LA PROCESADORA NACIONAL DE ALIMENTOS PRONACA", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Sangolquí, 23 de enero 2015

Ing. Rodolfo Fabián Morales A.

DEDICATORIA

A Dios, que me ha dado las fuerzas para poder cumplir una más de las metas trazadas para mi vida; a mis padres Alfonso y Margoth que con su cariño, amor y paciencia me han sabido guiar por el camino correcto; a mis hermanas Jenny y Cristina; y sobrino Anthony que con su apoyo y desinterés han estado siempre a mi lado apoyándome en cada decisión que he tomado.

AGRADECIMIENTOS

A Dios, que me ha dado sabiduría e inteligencia desde el inicio de este emprendimiento hasta el final y así culminar con éxito este reto trazado hace tiempo atrás.

A PRONACA, que es el lugar donde laboro diariamente, y que me ha facilitado y abierto las puertas, para el desarrollo del presente proyecto, brindándome la apertura que necesite para el desarrollo de mi tesis.

Al Ing. Daniel Altamirano, que gracias a su valioso aporte, tiempo y dirección pudimos concluir de manera exitosa la elaboración del presente proyecto.

A mis familiares y amigos, que de una u otra forma estuvieron presentes brindándome su apoyo durante todo el proceso de desarrollo y finalización de un logro más en mi vida.

Fabián

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El objetivo del presente proyecto, se ha enfocado en el desarrollo de un sistema de gestión de seguridad de la información, basada en tres dominios de las normas ISO 27001 e ISO 27002, para el área de Software de la Procesadora Nacional de Alimentos (PRONACA). Basados en un análisis de las políticas y normas existentes en PRONACA, se ha propuesto que los dominios a ser desarrollados son los siguientes: Control de acceso, que permitirá tener la información de la empresa siempre disponible, confiable y segura a través de la implementación de nuevas políticas. Adquisición, desarrollo y mantenimiento de los sistemas de información, que mantendrá controlados los sistemas y aplicaciones con las cuales cuenta actualmente la compañía y los que continúe adquiriendo, para el desarrollo de sus procesos diarios. Gestión de incidentes en la seguridad de la información, que controlará los incidentes que se puedan presentar en la seguridad de la información, evitando que estos incidentes se conviertan en vulnerabilidades que desencadenen en riesgos para la organización, ocasionando pérdidas importantes y provocando inestabilidad en sus procesos.

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 on three domains of the ISO 27001 and ISO 27002 standards for the area of Software of the National Food Processing (PRONACA). Based on an analysis of existing policies and standards PRONACA, it has been proposed that the domains to be developed are: Access Control, which will permit the company information always available, reliable and secure through the implementation of new policies. Acquisition, development and maintenance of information systems that maintain controlled systems and applications which currently has the company and continue acquiring, for the development of their daily processes. Incident Management in Information Security, which will control the incidents that may arise in information security, preventing these incidents become vulnerabilities that trigger on risks to the organization, causing major losses and instability in their processes.

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

CAPITULO I
INTRODUCCIÓN

1.1 Generalidades.

Existen técnicas de evaluación que permiten medir los controles y procedimientos informáticos que se encuentran definidos en una organización, mediante los cuales se puede identificar insolvencias para sugerir sus correcciones, bajo los estándares recomendados en las normas internacionales ISO 27001 e ISO 27002 en el área de la Gestión de la Seguridad Informática, centrándonos en los controles de accesos, adquisición, desarrollo y mantenimiento de software y concluir con la gestión de incidentes de seguridad de la información.

Mediante la investigación de campo que se realizará durante el desarrollo del proyecto de tesis, permitirá definir recomendaciones de los tres dominios de la norma ISO 27002, que son: control de accesos, mediante el cual se puede asegurar y controlar el no acceso a usuarios no autorizados al sistema ó sistemas; la adquisición, desarrollo y mantenimiento de los sistemas de información, encargado de mantener un análisis y justificación, para desarrollar o adquirir un sistema; y como tercer dominio la gestión de incidentes de seguridad de la información, que consiste en elaborar procesos de mejora continua que serán aplicados de acuerdo a la gestión de los incidentes encontrados.

Las normas ISO 27001 e ISO 27002; recomienda métodos de control que encaminan de la manera más concreta para lograr su objetivo, dependiendo de la compañía que la quiera aplicar, 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, agroindustrial y acuacultura.

Es una empresa comprometida con el mejoramiento de la calidad de vida de sus consumidores, clientes y colaboradores. Trabaja todos los días en la elaboración de productos confiables, ofrece miles de fuentes de trabajo digno y apoya al desarrollo de las zonas rurales del país.

PRONACA es una empresa ecuatoriana, que goza de confianza y aceptación dentro y fuera del país. Es una organización que contribuye a mejorar la productividad agrícola e industrial del Ecuador.

Por el gran tamaño y magnitud de la compañía es de suma importancia el tener la información protegida y disponible en todo tiempo, para lo cual se debe establecer políticas y controles de Seguridad Informática, que sean capaces de evitar en lo posible las amenazas constantes que puedan afectar a los sistemas y vulnerar dicha información.

1.3 Planteamiento del problema.

PRONACA, al ser una compañía que se dedica a la producción de alimentos para consumo humano y balanceado para animales, que se encuentra a nivel nacional, con sus oficinas matrices ubicadas en la ciudad de Quito-Ecuador, centros de distribución y plantas productoras en diferentes sitios de nuestro país, siendo muy importante el mantener la comunicación entre los usuarios de cada centro a través de aplicaciones y sistemas que tiene 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 mediante medidas preventivas y reactivas según estándares internacionales, que permitan resguardar y proteger la información, además no tiene una estructura establecida al momento de adquirir y realizar el mantenimiento de los Sistemas con la que cuenta la compañía, ya que el

volumen de transaccionalidad diario es muy alto, provocando de esta manera que las bases de datos se llenen a cada momento dejando inactivos los sistemas por varios minutos, lo cual desencadena en un malestar al usuario y retrasos en el despacho de la producción.

1.4 Justificación e importancia.

PRONACA, se verá beneficiada de este proyecto de tesis, que abarca tres dominios de las Normas Internacionales ISO 27001 e ISO 27002, ya que se realizará con el fin de implementar un Sistema de Gestión de Seguridad de la Información [SGSI], en el área de Software, de manera que permita obtener confiabilidad y disponibilidad al momento de ejecutar o interactuar con los Sistemas tanto internos como externos que usa la compañía, ya que por el momento no cuenta con políticas internacionales de SGSI, recomendados por la norma ISO 27001 e ISO 27002.

La falta de establecer políticas de seguridad de la información, repercute en varios factores que se los podría minimizar, como son, el tiempo de respuesta ante eventualidades con los sistemas y aplicaciones de la compañía, posibles ataques internos y externos afectando la privacidad de la Información. Dicha información es un activo sumamente importante, ya que en los sistemas o aplicaciones están las fórmulas de los distintos productos que ofrece la compañía tanto para consumo humano como animal, a mas de estudios de mercadeo, estadísticas, informes contables, financieros y proyectos desarrollados ó en proceso de desarrollo; por este motivo es imprescindible contar con políticas claramente establecidas para evitar el acceso de personas malintencionadas a esta información, ya que pueden perjudicar en gran manera a la compañía, provocando daños de un valor incalculable, con grandes consecuencias financieras e intelectuales.

Para PRONACA es importante el desarrollo de este proyecto de tesis, ya que con la implementación del SGSI, pondría continuar con las operaciones de manera confiable y segura, sabiendo que su información y accesos

cuentan con las debidas seguridades recomendadas por un estándar internacional, como lo es la ISO 27001.

1.5 Objetivos.

1.5.1 Objetivo General.

Diseñar un SGSI de tres dominios basada en la norma ISO 27001 e ISO 27002, para el área de Software de PRONACA.

1.5.2 Objetivos específicos.

- Determinar la situación actual de las políticas de seguridad de PRONACA.
- Describir el proceso de especificación y diseño de un Sistema de Gestión de Seguridad de la Información, desde su inicio hasta la producción de los planes de implementación.
- Elaborar la propuesta de un SGSI en base a los estándares ISO 27001 e ISO 27002.
- Presentar al director de TI de la compañía, para la puesta en marcha de la implementación de las políticas para un SGSI.

1.6 Alcance.

Este proyecto de tesis cubrirá el diseño de políticas de seguridad para PRONACA, con todos los lineamientos que exige la implementación de un SGSI según la Norma Internacional ISO 27001 e ISO 27002, centrándose en tres de sus dominios que son los siguientes:

- Control de acceso.
- Adquisición, desarrollo y mantenimiento de los Sistemas de información.
- Gestión de seguridad de la información.

Los resultados de este proyecto de tesis, servirán para que los usuarios de PRONACA, por medio de la Gerencia de Operaciones, estén en capacidad de aplicar las recomendaciones dadas por esta Norma

Internacional de Gestión de Seguridad de la Información, de manera oportuna, elevando de esta manera los niveles de seguridad y confiabilidad en sus Sistemas, estableciéndolas como políticas internas de la compañía.

CAPITULO II
MARCO TEORÍCO

2.1 Introducción.

En el Ecuador, al igual que en el resto del mundo las compañías consideran la información como un activo sumamente importante, dándole prioridad y buscando maneras de controlar los accesos de manera muy cuidadosa, a mas de buscar maneras de tenerla disponible en cualquier momento y actualizada en los distintos sistemas que puedan tener cada empresa.

Es por eso que se ha venido buscando maneras de obtener la mejor combinación entre la tecnología y la gestión de usuarios, que son los encargados de establecer políticas de seguridad, guiándose en estándares propuestos por entes regulatorios, que proveen de herramientas y recomendaciones para llegar a tener un control eficaz y eficiente de la información, jugando un papel muy importante la adquisición, mantenimiento y desarrollo de aplicaciones de las compañías.

2.2 Definición de seguridad de la información.

La información de una empresa, tiene un valor incalculable e importante para ella, por lo que es de suma importancia el mantenerla protegida y fuera del alcance de personas malintencionadas que quieran hacer un mal uso de dicha información.

Debido a que la información puede ser presentada en diversas formas como: impresa, video, audio, cintas, almacenada en algún dispositivo electrónico, etc., es necesario conservarla de una manera muy cuidadosa y segura, para que pueda ser utilizada en cualquier tiempo de manera confiable.

Es importante mencionar que la seguridad total de la información no existe, pero se han establecido diversas maneras y estándares que ayudan a

mitigar en lo posible los riesgos que constantemente se puedan ir presentando, minimizando estos riesgos a un nivel aceptable, es por eso que se recomienda mantener un constante control y mejoramiento de los procesos de seguridad de la información de manera continua.

La gestión eficaz de la seguridad de los sistemas de información es un aspecto primordial para salvaguardar a las organizaciones de los riesgos e inseguridades que pueden dañar de forma importante sus sistemas de información (UNIT, 2005).

La seguridad de la información en resumen es el conjunto de medidas preventivas y reactivas que las organizaciones y los sistemas tecnológicos permiten resguardar y proteger, lo cual lo pueden hacer por medio de la implementación apropiada de controles, políticas, procedimientos, normas, etc., que buscan la manera de obtener la confidencialidad, la disponibilidad e integridad de dicha información.

- **Confidencialidad.-** es permitir el acceso a la información únicamente a las personas que cuenten con la debida autorización, impidiendo la divulgación ó acceso a personas ó sistemas no autorizados.
- **Disponibilidad.-** la cualidad de la información de mantenerse a disposición de personas ó aplicaciones autorizadas, en el momento que la requieran.
- **Integridad.**- este atributo 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 en un tema sumamente importante cuando se habla de seguridad de la información, es por eso que la Norma ISO 27001 con todos sus controles, trata de mitigar al máximo los riesgos que se puedan presentar en la gestión de la información, sugiriendo que se debería

seleccionar estos controles de la norma, en base al resultado de un análisis previo de riesgos al que está expuesta la compañía y de esta manera conseguir una efectiva gestión de control de los riesgos.

2.3.1 Concepto de Riesgo.

Riesgo es la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información ó grupo de ellas (SGS, 2013).

2.3.2 Evaluar los riesgos de la seguridad de la información.

La gestión de los riesgos de la seguridad de la información requiere una evaluación apropiada de los riesgos y un método de tratamiento del riesgo que puede incluir una estimación de costos y beneficios, requerimientos legales y aspectos sociales, económicos y ambientales, las preocupaciones de las partes involucradas, prioridades, y otras entradas y variables según sea apropiado.

Los resultados de la evaluación de los riesgos de la seguridad de la información ayudarán a guiar y determinar las decisiones de gestión apropiadas para el tratamiento de acciones y priorización de la gestión de los riesgos de la seguridad de la información y para la implementación de los controles de seguridad pertinentes para protegerla contra estos riesgos (ISO/IEC, Técnicas de la seguridad, 2009).

2.3.3 Análisis del riesgo.

El propósito de la identificación del riesgo es determinar que podría suceder que se cause una pérdida potencial, y llegar a comprender 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, vulnerabilidades y consecuencias (INCONTEC, 2008).

2.3.4 Proceso de gestión del riesgo.

Como podemos ver en la Fig. 2.1, la constante comunicación y consulta son de doble vía con el hecho de establecer, identificar, analizar, evaluar y tratar los riesgos, para llegar a una valoración de los mismos, que juntamente con el adecuado monitoreo y revisión, se podría llegar a establecer claramente cuáles son los riesgos y tenerlos controlados para evitar que puedan desencadenar en una acción que ponga en riesgo la información y por ende las operaciones de la empresa.

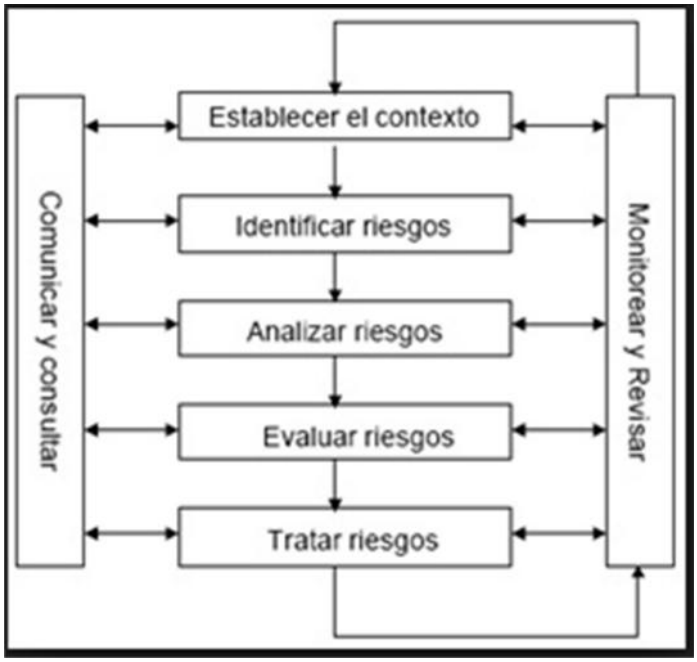

Figura 1 Proceso de gestión del riesgo **(SGS, 2013)**

La norma ISO 27001 especifica que los controles implementados dentro del alcance, los límites y el contexto del SGSI se deben basar en el riesgo. La aplicación de un proceso de gestión del riesgo en la seguridad de la información puede satisfacer este requisito. Existen muchos enfoques mediante los cuales se puede implementar exitosamente el proceso en una organización. La organización debería utilizar cualquier enfoque que se ajuste mejor a sus circunstancias para cada aplicación específica del proceso (INCONTEC, 2008).

En un SGSI se han establecido los siguientes procesos:

- **Planificar.-** es el establecimiento del contexto, la valoración del riesgo, el desarrollo del plan de tratamiento del riesgo y la aceptación del riesgo.
- **Hacer.-** en esta fase es en donde se implementan las acciones y los controles que son necesarios para reducir el riesgo hasta un nivel aceptable, de acuerdo con el plan de tratamiento del riesgo.
- **Verificar.-** los directores determinarán la necesidad de revisiones de las valoraciones y del tratamiento del riesgo a la luz de los incidentes y los cambios en las circunstancias.
- **Actuar.-** aquí es en donde se llevan a cabo todas las acciones que son necesarias, incluyendo la aplicación adicional del proceso de gestión del riesgo en la seguridad de la información.

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

Tabla 1 Fases del proceso del SGSI

Procesos de SGSI	Proceso de gestión del riesgo en la seguridad de la información
Planificar	Establecer el contexto. Valoración del riesgo. Planificación del tratamiento del riesgo. Aceptación del riesgo.
Hacer	Implementación del plan de tratamiento del riesgo.
Verificar	Monitoreo y revisión continuos de los riesgos.
Actuar	Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información

Fuente: (SGS, 2013).

2.3.5 Principios de gestión del riesgo.

Una de las maneras de identificar los riesgos es mediante un cuadrante, en el cual se debe colocar los riegos según corresponda su grado de

probabilidad de ocurrencia y la consecuencia que este traería, para de esta manera tenerlos claramente identificados y poder tomar acciones sobre ellos.

Los cuadrantes mostrados en la Figura 2.2 corresponden a las siguientes valoraciones:

- **Evitar.-** quiere decir que la probabilidad y la consecuencia son demasiado altos y se lo debe evitar de cualquier manera, ó de lo contrario el riesgo se convertirá en una grave amenaza; hay que buscar las maneras de pasarlo al cuadrante de Aceptables.

- **Transferir.**- es cuando la consecuencia es muy alta, pero la probabilidad es baja, es un riesgo más controlable, pero no se lo debe descuidar hasta que se consiga pasarlo al cuadrante Aceptable.

- **Reducir.-** la consecuencia es baja, pero la probabilidad es muy alta, es un riesgo manejable, pero de igual manera lo ideal sería que esté en el cuadrante de Aceptable.

- **Aceptar.-** son riesgos con los cuales se puede gestionar sin entorpecer los procesos, siempre y cuando sean monitoreados y no pasen a ninguno los otros tres cuadrantes, es decir el trabajo aquí es mantenerlos en este cuadrante.

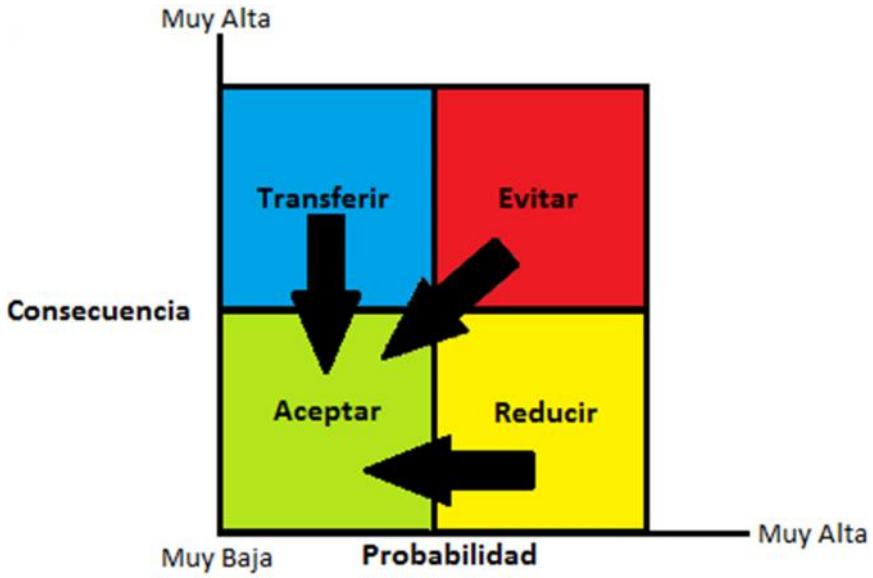

Figura 2 Principios de gestión del riesgo **(SGS, 2013)**.

2.3.6 Clasificación de los activos.

La información es considerada como uno de los activos más importantes que tiene una empresa o compañía, es por eso que deben estar claramente definidos y valorados estos activos, de acuerdo a los lineamientos de seguridad de cada organización.

Los activos han sido clasificados de la siguiente manera:

- Activos de información:
  - Base de datos.
  - Procedimientos.
  - Material de formación.
- Documentos en papel:
  - Inventarios.
  - Contratos.
- Activos de software:
  - Aplicaciones de software.
  - Software de sistema.
  - Herramientas “Case”.
- Activos físicos:

  - Ordenadores.
  - Fax.
  - Aparatos de aire acondicionado.
  - Edificios.
  - Dispositivos de red.
  - Bienes
- Personas:
  - Personal.
  - Clientes.
  - Suscriptores.
- Servicio:
  - Calefacción.
  - Red.
  - Telecomunicaciones.
  - Energía.
  - Aire acondicionado.
  - Agua corriente.
- Intangibles:
  - Buena voluntad / reputación.
  - Confianza en la organización.
  - Imagen corporativa.
- Dinero (SGS, 2013).

2.3.7 Criterios Básicos de la gestión del riesgo.

Dependiendo del alcance y los objetivos de la gestión del riesgo, se pueden aplicar diferentes enfoques, abordando criterios básicos como los siguientes:

Criterios de evaluación del riesgo.

Es recomendable 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:

- El valor estratégico del proceso de información del negocio.
- La criticidad de los activos de información involucrados.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- La importancia de la disponibilidad, confidencialidad e integridad para las operaciones del negocio.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación.

Criterios de impacto.

Se recomienda desarrollar criterios de impacto del riesgo y especificarlos en términos del grado de daño o de los costos para la organización, causados por un evento de seguridad de la información, considerando los siguientes aspectos:

- Nivel de clasificación de los activos de información afectados.
- Brechas en la seguridad de la información, cuando se pueda perder la confidencialidad, integridad y disponibilidad.
- Operaciones deterioradas.
- Pérdida del negocio y del valor financiero.
- Alteración de planes y fechas límites.
- Incumplimiento de los requisitos legales, reglamentarios o contractuales.

Criterios de la aceptación del riesgo.

Es recomendable desarrollar y especificar criterios de aceptación del riesgo. Estos criterios dependen con frecuencia de las políticas, metas objetivos de la organización y de las partes interesadas, se debería considerar los siguientes aspectos:

- Los criterios de aceptación del riesgo pueden incluir umbrales múltiples, con una meta de nivel de riesgo deseable, pero con disposiciones para que la alta dirección acepte los riesgos por encima de este nivel, en circunstancias definidas.

- Los criterios de aceptación del riesgo se pueden expresar como la relación entre el beneficio estimado y el riesgo estimado.
- Los diferentes criterios de aceptación del riesgo se pueden aplicar a diferentes clases de riesgos.
- Los criterios de aceptación del riesgo pueden incluir requisitos para 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.

Los criterios de aceptación del riesgo se pueden definir de acuerdo con la expectativa de duración que se tenga del riesgo, para lo cual se debería considerar elementos tales como: criterios del negocio, aspectos legales y reglamentarios, operaciones, tecnología, finanzas, factores sociales y humanitarios (INCONTEC, 2008).

2.3.8 El alcance y límites del riesgo.

El alcance y los límites de la gestión del riesgo, deberían ser definidos por la organización, para garantizar que todos los activos se tomen en cuenta en la valoración del riesgo. Para esto es necesario tener la suficiente información acerca de la organización, para determinar el ambiente en que ella funciona y establecer la pertinencia de la información para el proceso de gestión de riesgo en la seguridad de la información.

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

- Los objetivos estratégicos de negocio, políticas y estrategias de la organización.
- Procesos del negocio.
- Las funciones y estructura de la organización.
- Los requisitos legales, reglamentos y contractuales aplicables a la organización.
- La política de seguridad de la información de la organización.

- El enfoque global de la organización hacia la gestión del riesgo.
- Activos de información.
- Ubicación de la organización y sus características geográficas.
- Restricciones que afectan a la organización.
- Expectativas de las partes interesadas.
- Entorno sociocultural.
- Interfaces.

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

2.3.9 Identificación del riesgo.

El propósito de la identificación del riesgo es determinar que podría suceder 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.

Es importante identificar los activos de la organización, un activo es todo aquello que tiene valor para dicha organización y que por lo tanto requiere de cuidado y protección, para definir todos los activos, es necesario tomar en cuenta que el sistema de información consta de más elementos que solo hardware y software. La identificación de los activos se debería llevar a cabo con un nivel adecuado de detalle, que proporcione información suficiente para la valoración del riesgo. Es importante tener bien identificado al propietario de cada activo, para asignarle responsabilidad y rendición de cuentas sobre este, el responsable del activo, puede no tener derechos de propiedad sobre este activo, pero tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad, según corresponda.

2.3.10 Identificación de las vulnerabilidades.

Vulnerabilidades.- son puntos débiles que al ser explotados por amenazas, afectan la confidencialidad, disponibilidad e integridad de la información de un individuo o empresa. Uno de los primeros pasos para la implementación de la seguridad es rastrear y eliminar los puntos débiles de un ambiente de tecnología de la información. Al ser identificados los puntos débiles, será posible dimensionar los riesgos a los cuales el ambiente está expuesto y definir las medidas de seguridad apropiadas para su corrección.

Amenazas.- Son agentes capaces de explotar los fallos de seguridad que denominamos puntos débiles y, como consecuencia de ello, causar pérdidas o daños a los activos de una organización. Los activos están constantemente sometidos a amenazas que pueden colocar en riesgo la integridad, confidencialidad y disponibilidad de la información. Estas amenazas siempre existirán y están relacionadas a causas que representan riesgos, las cuales pueden ser: causas naturales o no naturales, causas internas o externas. Uno de los objetivos de la seguridad de la información es impedir que las amenazas exploten puntos débiles y afecten alguno de los principios básicos de la seguridad de la información (integridad, disponibilidad, confidencialidad), causando daños al negocio de las empresas. Las amenazas son constantes y pueden ocurrir en cualquier momento (Jaimes, 2009).

Las amenazas siempre han existido y es de esperarse que conforme avance la tecnología también surgirán nuevas formas en las que la información puede llegar a estar expuesta.

Para identificar las vulnerabilidades, debemos hacer una lista de amenazas conocidas, juntamente con los activos y controles existentes, para identificar de esta manera las vulnerabilidades que puedan ser

explotadas por las amenazas y que podrían causar daños a los activos de la organización.

En las áreas 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 sola presencia de una vulnerabilidad no causa daño por sí misma, dado que es necesario que haya una amenaza presente para explotarla. Una vulnerabilidad que no tiene una amenaza correspondiente puede no requerir de la implementación de un control, pero es recomendable reconocerla y monitorearla para determinar los cambios. Por el contrario una amenaza que no tiene una vulnerabilidad correspondiente puede no resultar un riesgo (INCONTEC, 2008).

2.3.11 Reducción del Riesgo.

Al riesgo se lo debería reducir lo máximo posible hasta llegar a tener un riesgo residual aceptable, que es el resultado que se obtendría después de haber trabajado con el riesgo aplicando o tomando medidas, que estarán determinadas en un plan de seguridad de la información, el cual será aplicado en nuestro ambiente de producción, después de haber sido certificado y probado en un ambiente de desarrollo.

Es recomendable seleccionar controles adecuados, y considerar varios aspectos tales como: costos y tiempo para la implementación de estos controles, a más de los aspectos técnicos, ambientales y culturales, ya que con frecuencia de esta selección dependerá la reducción de las inversiones totales, además es indispensable entender con claridad que se debe tener disponibles valores para la adquisición, implementación, administración, operación, monitoreo y mantenimiento de los controles, en comparación con el valor de los activos que se protegerán.

Es importante la implementación de los controles, ya que pueden brindar uno ó más de los siguientes tipos de protección: corrección, eliminación, prevención, minimización del impacto, disuasión, detección, recuperación, monitoreo y toma de conciencia.

2.3.12 Monitoreo y revisión de los factores de riesgo.

Los riesgos no son estáticos, las amenazas y vulnerabilidades ó las consecuencias pueden cambiar de manera repentina sin ninguna indicación, por tal motivo, es necesario el constante monitoreo para que se puedan detectar estos cambios, por este motivo las organizaciones deberían garantizar el continuo monitoreo de los siguientes aspectos:

- Activos nuevos que se han incluido en el alcance de la gestión de riesgo.
- Modificaciones necesarias de los valores de los activos, puede ser por cambios en los requisitos de los negocios.
- Nuevas amenazas que podrían estar activas tanto fuera como dentro de la organización y que no se han valorado.
- Probabilidad de que nuevas vulnerabilidades o el incremento en las vulnerabilidades existentes, permitan que las amenazas exploten.
- Vulnerabilidades identificadas para determinar aquellas que se exponen a nuevas amenazas o que vuelven a surgir.

- El incremento en el impacto o las consecuencias de las amenazas evaluadas, las vulnerabilidades y los riesgos en conjunto que dan como resultado un nivel aceptable de riesgo.
- Incidentes de 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).

2.3 Normas ISO 27000.

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

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

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

2.3.1 Origen.

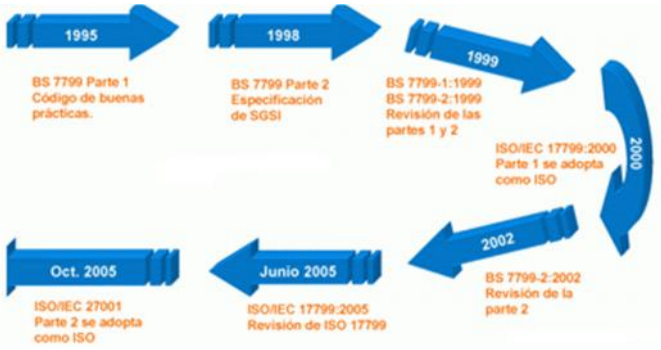

Figura 3 Historia de ISO 27001. **(ISO2700.ES, 2012)**.

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

- 1979 Publicación BS 5750 - ahora ISO 9001.
- 1992 Publicación BS 7750 - ahora ISO 14001.
- 1996 Publicación BS 8800 - ahora OHSAS 18001.

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

La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.
En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

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

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

2.3.2 Definición de las normas ISO 27000.

La serie ISO 27000 es una familia de estándares internacionales, que a semejanza de otras normas tiene rangos de numeración reservados por ISO que van de la 27000 a 27019 y de 27030 a 27044.

ISO 27000.

Esta norma internacional provee una visión general de los sistemas de gestión de la seguridad de la información, que conforman el objeto del grupo de normas de SGSI y contiene términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión. Esta norma es gratuita, a diferencia de las demás de la serie, que tienen costo (ISO/IEC, Descripción general y vocabulario, 2009).

ISO 27001.

Publicada el 15 de Octubre de 2005, es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información.

Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que

sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados (ISO27000.es, 2005).

ISO 27002.

Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005. Actualmente, este estándar se encuentra en periodo de revisión en el subcomité ISO SC27, con fecha prevista de publicación de la segunda edición en Mayo de 2014 (ISO27000.es, 2005).

ISO 27003.

El propósito de esta norma es proporcionar orientación práctica ó directrices en el desarrollo del plan de implementación para un sistema de Gestión de Seguridad de la Información, dentro de una organización en conformidad con la ISO/IEC 27001:2008, la implementación efectiva de un SGSI es generalmente ejecutada como un proyecto.

Mediante el uso de esta norma la organización será capaz de de desarrollar un proceso para la gestión de la seguridad de la información brindando a las partes interesadas garantía de que los riesgos para los activos de información se mantienen continuamente dentro de los límites aceptables de seguridad de la información según lo definido por la organización. Esta norma no es certificable (INDECOPI, 2012).

ISO 27004.

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

ISO 27005.

Publicada en segunda edición el 1 de Junio de 2011 (primera edición del 15 de Junio de 2008). No certificable. Esta norma proporciona directrices para la gestión del riesgo en la seguridad de la información en una organización, dando soporte particular a los requisitos de un Sistema de Gestión de Seguridad de la Información, de acuerdo con la norma NTC-ISO/IEC 27001.

Sin embargo, esta norma no brinda ninguna metodología específica para la gestión del riesgo en la seguridad de la información. Corresponde a la organización definir su enfoque para la gestión del riesgo, dependiendo por ejemplo del alcance de su SGSI, del contexto de la gestión del riesgo o del sector industrial. Se puede utilizar una variedad de metodologías existentes bajo la estructura descrita en esta norma para implementar los requisitos de un sistema de gestión de seguridad de la información.

Esta norma es pertinente para los directores y el personal involucrado en la gestión del riesgo en la seguridad de la información dentro de la organización y, cuando corresponda, para las partes externas que dan soporte a dichas actividades.

Además apoya los conceptos generales especificados en la norma ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación

satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos (INCONTEC, 2008).

ISO 27006.

Publicada en segunda edición el 1 de Diciembre de 2011 (primera edición del 1 de Marzo de 2007). Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información, los requisitos específicos relacionados con ISO 27001:2005 y los SGSI. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma (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 complemento a lo especificado en ISO 19011.

ISO 27011.

Esta norma consiste en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones).

ISO 27031.

La norma fue publicada el 01 de Marzo de 2011. No es certificable. Es una guía de apoyo para la adecuación de las tecnologías de información y comunicación (TIC) de una organización para la continuidad del negocio.

ISO 27032.

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

concretamente: Información de seguridad, seguridad de las redes, seguridad en Internet e información de protección de infraestructuras críticas (CIIP).

Cubre las prácticas de seguridad a nivel básico para los interesados en el ciberespacio. Esta norma establece una descripción general de Seguridad Cibernética, una explicación de la relación entre la ciberseguridad y otros tipos de garantías, una definición de las partes interesadas y una descripción de su papel en la seguridad cibernética, una orientación para abordar problemas comunes de Seguridad Cibernética y un marco que permite a las partes interesadas a que colaboren en la solución de problemas en la ciberseguridad.

ISO 27034.

Norma dedicada a la seguridad en aplicaciones informáticas, consistente en las siguientes 6 partes:

- **27034-1.-** conceptos generales.
- **27034-2.-** marco normativo de la organización.
- **27034-3.-** proceso de gestión de seguridad en aplicaciones.
- **27034-4.-** validación de la seguridad en aplicaciones.
- **27034-5.-** estructura de datos y protocolos y controles de seguridad de aplicaciones.
- **27034-6.-** guía de seguridad para aplicaciones de uso específico.

ISO 27799.

Publicada el 12 de Junio de 2008. Es una norma que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002:2005, en cuanto a la seguridad de la información sobre los datos de salud de los pacientes. Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215 (ISO2700.ES, 2012).

2.3.3 Estándar ISO/IEC 27001.

Generalidades.

Esta norma ha sido elaborada para brindar un modelo que permitirá obtener el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un SGSI. La adopción de dicho SGSI debería ser una decisión estratégica tomada por la organización. El diseño e implementación del SGSI están influenciados por las necesidades y objetivos, requisitos de seguridad, procesos empleados y el tamaño y estructura de la organización, se espera que estos aspectos y sus sistemas de apoyo cambien con el tiempo, ajustándose de acuerdo a las necesidades de la organización.

Esta norma se puede usar para evaluar la conformidad, por las partes interesadas, tanto internas como externas.

Enfoque basado en procesos.

Esta norma promueve la adopción de un enfoque basado en procesos, para funcionar eficazmente una organización debe identificar y gestionar muchas actividades. Se puede considerar como un proceso cualquier actividad que use recursos y cuya gestión permita la transformación de entradas en salidas, con frecuencia el resultado de un proceso constituye directamente la entrada del proceso siguiente.

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

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

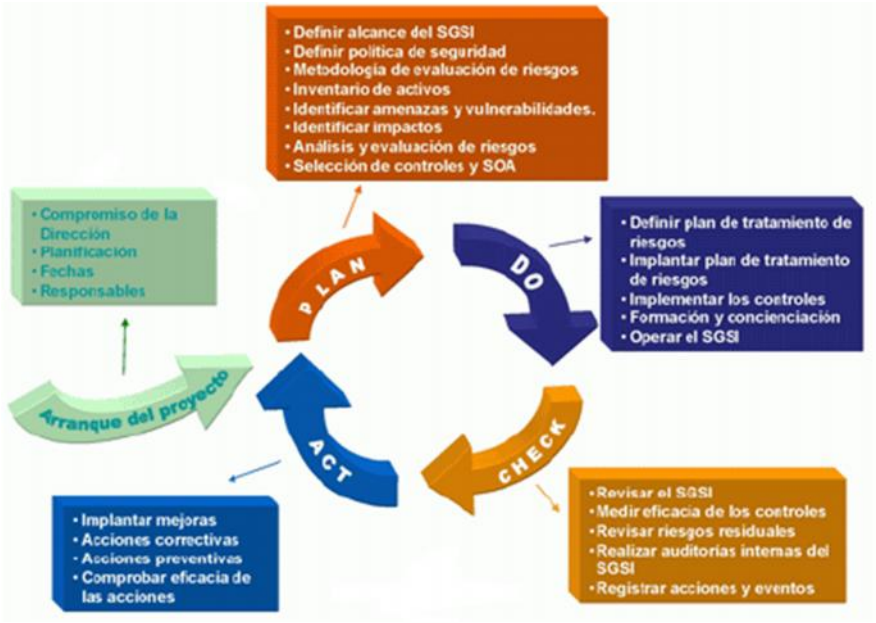

Figura 4 Ciclo de adaptación de la Norma **(SGS, 2013)**.

Como podemos ver en la figura 4, el ciclo PHVA, está compuesto por los siguientes términos que significan:

- **Planear (P).-** consiste en establecer políticas, objetivos, procesos, procedimientos y metas pertinentes para gestionar el riesgo y mejorar la seguridad de la información con el fin de entregar indicadores de resultados y establecer la manera (el camino, el método) para alcanzar las metas propuestas por una organización.
- **Hacer (H ó D).-** es la ejecución de las tareas exactamente de la forma prevista en el plan y en la recolección de datos para la verificación del proceso. En esta etapa es esencial el entrenamiento en el trabajo resultante de la fase de planeamiento.
- **Verificar (V ó C).-** tomando como base los datos recolectados durante la ejecución, se compara el resultado obtenido con la meta planificada.
- **Actuar (A).-** Esta es la etapa en la cual el usuario detectó desvíos y actuará de modo que el problema no se repita nunca más, es decir tomar acciones correctivas y preventivas con base en los resultados de la auditoría interna y la revisión por la dirección, para lograr la mejora continua del SGSI (Universidad de Colombia, 2012).

Tecnología de la Información – Técnicas de Seguridad - Sistema de Gestión de Seguridad de Información - Requisitos.

- **Generalidades.**

Es importante mencionar que esta norma no pretende incluir todas las disposiciones necesarias, para elaborar un contrato, ya que los usuarios son los directos responsables de su correcta aplicación.

El cumplimiento con una norma en sí misma no confiere excepción de las obligaciones legales.

- La norma internacional ISO 27001, es aplicable a todo tipo de organización.
- La norma específica los requisitos para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI, documentado dentro del contexto de los riesgos globales del negocio de la organización.
- Especifica los requisitos para la implementación de controles de seguridad adaptados a las necesidades de las organizaciones individuales ó a partes de ellas.
- El SGSI está diseñado para seleccionar controles suficientes y proporcionales que protejan los activos de información y brinden confianza a las partes interesadas.

- **Aplicación.**

Los requisitos establecidos en esta norma son genéricos y están previstos para ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño y naturaleza. Cualquier exclusión de controles, considerada necesaria para satisfacer los criterios de aceptación de riesgos, necesita justificarse y debe suministrarse evidencia de que los riesgos asociados han sido aceptados apropiadamente por las personas responsables. Si se llega a excluir cualquier control, las declaraciones de conformidad con esta norma no son aceptables a menos que dichas exclusiones no afecten la capacidad de la organización y la responsabilidad

para ofrecer seguridad de la información que satisfaga los requisitos de seguridad determinados por la valoración de riesgos y los requisitos reglamentarios aplicables (SGS, 2013).

- **Términos y definiciones.**

Esta norma al igual que cualquier otra, usa términos y definiciones, con los que se trabajará durante el desarrollo del proyecto.

- **Aceptación de riesgo.-** decisión de asumir el riesgo.
- **Activo.-** cualquier cosa que tiene valor para la organización.
- **Análisis de riesgo.-** uso sistemático de la información para identificar las fuentes y estimar el riesgo.
- **Confidencialidad.-** propiedad que determina la condición de que la información no esté disponible ni sea relevada a individuos ó procesos no autorizados.
- **Control.-** medios para manejar el riesgo, incluyen políticas, procedimientos, lineamientos, prácticas ó estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión ó de naturaleza legal.
- **Declaración de aplicabilidad.-** documento que describe los objetivos de control y los controles pertinentes aplicables para el SGSI de la organización.
- **Disponibilidad.-** que la información sea accesible y utilizable por solicitud de una entidad autorizada.
- **Evaluación de riesgo.-** proceso de comparar el riesgo estimado contra el criterio de riesgo dado, para determinar la importancia del riesgo.
- **Gestión de riesgo.-** actividades coordinadas para dirigir y controlar una organización en relación con el tiempo.
- **Integridad.-** propiedad de proteger la exactitud y estado completo de los activos.
- **Incidente de seguridad de la información.-** es un evento ó serie de eventos de seguridad de la información no deseados ó inesperados,

que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Lineamiento.-** una descripción que aclara qué se debería hacer y cómo, para lograr los objetivos propuestos.
- **Política.-** intención y dirección general expresada formalmente por la gerencia.
- **Riesgo.-** combinación de la probabilidad de un evento y su concurrencia.
- **Riesgo residual.**- nivel restante de riesgo después del tratamiento de riesgo.
- **Seguridad de la información.-** preservación de la confidencialidad, integridad y disponibilidad de la información, además de la involucra la autenticidad, trazabilidad y fiabilidad.
- **Sistema de seguridad de la información SGSI.-** parte del sistema de gestión global basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.
- **Amenaza.-** una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización.
- **Vulnerabilidad.-** la debilidad de un activo ó grupo de activos que puede ser explotada por una ó más amenazas.
- **Tratamiento de riesgo.-** proceso de selección e implementación de medidas para modificar el riesgo.
- **Valoración del riesgo.-** proceso global de análisis y evaluación del riesgo (SGS, 2013).
- **Sistema de Gestión de seguridad de la información.**

La organización debe establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI, en el contexto de las actividades globales del negocio de la organización y de los riesgos que enfrenta.

Para establecer un SGSI, la organización, debe cumplir con los siguientes puntos:

a) Definir el alcance y límites del SGSI en términos de características del negocio, la organización, su ubicación, sus activos y tecnología, e incluir los detalles y justificación de cualquier exclusión del alcance.
b) Definir una política del SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología, que incluya un marco de referencia para fijar sus objetivos, tener en cuenta los requisitos del negocio, alineación con el contexto organizacional estratégico de gestión de riesgo, criterios de evaluación de riesgos y aprobación por la dirección.
c) Definir el enfoque organizacional hacia la valoración del riesgo.
d) Identificar los riesgos.
e) Análisis y evaluación de los riesgos.
f) Identificar y evaluar las operaciones para el tratamiento de los riesgos.
g) Seleccionar los objetivos de control y controles para el tratamiento de los riesgos.
h) Obtener la aprobación de la dirección sobre los riesgos residuales propuestos.
i) Obtener la aprobación de la dirección para implementar y operar el SGSI.
j) Elaborar una declaración de aplicabilidad, que contenga objetivos y de control y controles, y exclusiones con sus respectivas justificaciones (SGS, 2013).

Para logra la implementación y operación del SGSI, la organización debe realizar lo siguiente:

a) Implementar las mejoras identificadas en el SGSI.
b) Emprender las acciones correctivas y preventivas.
c) Comunicar las acciones y mejoras a todas las partes interesadas.
d) Asegurar que las mejoras logren los objetivos previstos.

- **Responsabilidad de la dirección.**

La dirección debe comprometerse a brindar evidencia de su responsabilidad con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del SGSI:

a) Mediante el establecimiento de una política de SGSI.
b) Asegurando que se establezcan los objetivos y planes del SGSI.
c) Estableciendo funciones y responsabilidades de la seguridad de la información.
d) Comunicando a la organización la importancia de cumplir los objetivos de seguridad de la información e indicar la necesidad de mejora continua.
e) Brindando los recursos suficientes para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI.
f) Decidir los criterios para la aceptación de riesgos y los niveles de riesgo aceptables.
g) Asegurardo que se realizan auditorías internas del SGSI.
h) Efectuando las revisiones por la dirección del SGSI.

La organización debe determinar y suministrar los recursos necesarios para:

a) Establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI.
b) Asegurar que los procedimientos de seguridad de la información brindan apoyo a los requisitos del negocio.
c) Identificar y atender los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales.
d) Mantener la seguridad suficiente mediante la aplicación correcta de todos los controles implementados.
e) Llevar a cabo revisiones cuando sea necesario, y relacionar apropiadamente a los resultados de estas revisiones.
f) En donde se requiera, mejorar la eficacia del SGSI.

- **Auditorías internas al SGSI.**

La organización debe realizar auditorías internas al SGSI en intervalos planificados, para determinar si los objetivos de control, controles, procesos y procedimientos de su SGSI, cumplen según lo planificado.

Se debe planificar un programa de auditoría, tomando en consideración el estado e importancia de los procesos y áreas que se van a auditar, así como los resultados de auditorías previas. Se deben definir los criterios, alcance, frecuencia y métodos de auditoría (SGS, 2013).

- **Mejora del SGSI.**

La organización debe mejorar continuamente la eficiencia del SGSI mediante el uso de la política de seguridad de la información, los objetivos de la seguridad de la información, los resultados de la auditoría, el análisis de los eventos a los que se les ha hecho seguimiento, las acciones correctivas y preventivas y la revisión por la dirección.

Además se debe tener una acción correctiva, en donde la organización debe emprender acciones para eliminar la causa de no conformidades asociadas con los requisitos del SGSI, con el fin de prevenir que ocurran nuevamente.

Se concluirá con una acción preventiva, donde la organización determinará acciones para eliminar la causa de no conformidades potenciales con los requisitos del SGSI y evitar que ocurran. Las acciones preventivas tomadas deben ser apropiadas al impacto de los problemas potenciales. La organización debe identificar los cambios e identificar los requisitos en cuanto a acciones preventivas, concentrando la atención en los riesgos que han cambiado significativamente (SGS, 2013).

2.3.4 Estándar ISO/IEC 27002.

La ISO/IEC 17799 ó también llamada ISO 27002, es una guía de buenas prácticas en la gestión de la seguridad de la información, la cual contiene 39

objetivos de control y 133 controles que se encuentran agrupados en 11 dominios principales.

Alcance.

Con esta norma se podrá iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información dentro de una organización, después de haber realizado una evaluación de riesgos, la norma recomienda un conjunto de objetivos de control y controles a implementarse. Los objetivos delineados en este estándar internacional proporcionan un lineamiento general sobre los objetivos de gestión de seguridad de la información generalmente aceptados.

Dominios.

Cada dominio contiene objetivos y controles, como se muestra en la Tabla 2.2.

Tabla 2 Cláusulas Objetivos y Controles de la Norma ISO 27002.

	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

El orden de las cláusulas en este estándar no implica ni establece de ninguna manera su importancia, dependiendo de las circunstancias, todas las cláusulas pueden ser importantes, por lo tanto, cada organización que aplica este estándar debería identificar las cláusulas aplicables, cuán importante son y su aplicación a los procesos comerciales individuales (ISO27000.es, 2005).

Se aplicarán las recomendaciones de los dominios 7, 8 y 9 de la norma ISO 27002, para PRONACA.

Control de Acceso.

- **Requerimientos del negocio para el control del acceso.**

Objetivo 1: Controlar el acceso a la información. Se tendría que controlar el acceso a la información, medios de procesamiento de la información y procesos comerciales sobre la base de los requerimientos comerciales y de seguridad.

Las reglas de control del acceso deberán tomar en cuenta las políticas para la divulgación y autorización de la información.

a) Políticas de control del acceso.

Control 1.- Se deberá establecer, documentar y revisar la política de control de acceso en base a los requerimientos comerciales y de seguridad para el acceso.

- **Gestión de acceso del usuario.**

Objetivo 2: Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información.

Se deberían establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información. Los procedimientos tendrían que abarcar todas las etapas en el ciclo de vida del acceso del usuario, desde el registro inicial de usuarios

nuevos hasta el des-registro final de los usuarios que ya no requieren acceso a los sistemas y servicios de información. Cuando sea apropiado, se debe prestar atención especial a la necesidad de controlar la asignación de derechos de acceso privilegiados, lo que permite a los usuarios superar los controles del sistema.

a) Registro del usuario.

Control 2: debería existir un procedimiento formal para el registro y des-registro del usuario para otorgar y renovar el acceso a todos los sistemas y servicios de información.

b) Gestión de privilegios.

Control 3: se debería restringir y controlar la asignación y uso de privilegios.

c) Gestión de las claves secretas de los usuarios.

Control 4: La asignación de claves secretas se tendría que controlar a través de un proceso de gestión formal.

d) Revisión de los derechos de acceso del usuario.

Control 5: La gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.

- **Responsabilidades del usuario.**

Objetivo 3: Evitar el acceso de usuarios no-autorizados, evitar poner en peligro la información y evitar el robo de información y los medios de procesamiento de la información. La cooperación de los usuarios no autorizados es esencial para una seguridad efectiva.

Los usuarios deben estar al tanto de sus responsabilidades para mantener controles de acceso efectivos, particularmente con relación al uso de claves secretas y la seguridad del equipo del usuario. Se debe elaborar

políticas, las cuales serán aprobadas por el directorio de la compañía para su posterior difusión, en donde se pueda ver las obligaciones que tienen los usuarios acerca de escritorio y pantalla limpios para reducir el riesgo de acceso no autorizado o daño a los papeles y medios de procesamiento de la información.

a) Uso de claves secretas.

Control 6: se debe exigir a los usuarios que apliquen las políticas de la compañía y sigan las buenas prácticas de seguridad acerca del uso de claves secretas.

b) Equipo del usuario desatendido.

Control 7: los usuarios deben asegurar que su equipo cuando se quede sin la supervisión debe quedar con la seguridad apropiada.

c) Política de escritorio y pantalla limpios.

Control 8: se debería adoptar una política de escritorio limpio para papeles y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información (ISO27000.es, 2005).

- **Control de acceso a la red.**

Objetivo 4: Evitar el acceso no autorizado a los servicios de red. Se debería controlar el acceso a los servicios de redes internas y externas.

El acceso del usuario a las redes y servicios de las redes no tendrían que comprometer la seguridad de los servicios de la red asegurando:

a) Que existan las interfaces apropiadas entre la red de la organización y las redes de otras organizaciones y redes públicas.
b) Se apliquen los mecanismos de autenticidad apropiados para los usuarios y el equipo.
c) El control del acceso del usuario a la información debería ser obligatorio.

a) Política sobre el uso de los servicios de la red.

Control 9: Los usuarios sólo deberían tener acceso a los servicios para los cuales hayan sido específicamente autorizados.

b) Autenticación del usuario para las conexiones externas.

Control 10: Se deberían utilizar métodos de autenticación apropiados para controlar el acceso de usuarios remotos.

c) Identificación del equipo en las redes.

Control 11: La identificación automática del equipo se debe considerar como un medio para autenticar las conexiones de ubicaciones y equipos específicos.

d) Protección del puerto de diagnóstico y configuración remoto.

Control 12: Se debería controlar el acceso físico y lógico a los puertos de diagnóstico y configuración (ISO27000.es, 2005).

e) Segregación en redes.

Control 13: Los grupos de servicios de información, usuarios y sistemas de información deben ser segregados en redes.

f) Control de conexión a la red.

Control 14: Para las redes compartidas, especialmente aquellas que se extienden a través de las fronteras de la organización, se debería restringir la capacidad de los usuarios para conectarse a la red, en línea con la política de control de acceso y los requerimientos de las aplicaciones comerciales.

g) Control de routing de la red.

Control 15: Se debería implementar controles de routing en las redes para asegurar que las conexiones de la computadora y los flujos de

información no violen la política de control de acceso de las aplicaciones comerciales.

Si se emplean tecnologías proxy, se pueden utilizar los gateways de seguridad para validar las direcciones de la fuente y el destino en los puntos de control de las redes internas y externas. Los encargados de la implementación deberían estar al tanto de las fuerzas y debilidades de cualquier mecanismo empleado. Los requerimientos para el control del routing de la red se tendrían que basar en las políticas de control de acceso.

- **Control de acceso al Sistema Operativo.**

Objetivo 5: Evitar el acceso no autorizado a los sistemas operativos. Se debe utilizar medios de seguridad para restringir el acceso a los sistemas operativos a los usuarios autorizados. Los medios deberían tener la capacidad para:

a) Autenticar a los usuarios autorizados, en concordancia con una política de control de acceso definida.
b) Registrar los intentos exitosos y fallidos de autenticación del sistema.
c) Registrar el uso de los privilegios especiales del sistema.
d) Emitir alarmas cuando se violan las políticas de seguridad del sistema.
e) Proporcionar los medios de autenticación apropiados.
f) Cuando sea apropiado, restringir el tiempo de conexión de los usuarios.

a) Procedimientos para un registro seguro.

Control 16: El acceso a los sistemas operativos deberán ser controlados mediante los procedimientos de registro seguro, que existen en la compañía, llevando un control de cada incidencia que se pudiera presentar, para cual se llenarán formatos de registro establecidos en las políticas internas.

b) Identificación y autenticación del usuario.

Control 17: Todos los usuarios tienen un identificador único (ID de usuario) para su uso personal, y se debería escoger una técnica de autenticación adecuada para sustanciar la identidad de un usuario.

c) Sistema de gestión de claves secretas.

Control 18: Los sistemas para el manejo de claves secretas deben ser interactivas y además tienen que asegurar que estas claves secretas no puedan ser vulneradas ni extraídas por personas tanto internas como externas a la compañía.

d) Uso de las utilidades del sistema.

Control 19: Se debe restringir y controlar estrechamente el uso de los programas de utilidad que podrían ser capaces de superar los controles de los sistemas y las aplicaciones.

e) Cierre de una sesión por inactividad.

Control 20: Las sesiones inactivas tendían que ser cerradas después de un periodo de inactividad definido.

f) Limitación del tiempo de conexión.

Control 21: Se debe utilizar restricciones sobre los tiempos de conexión no mayores a 5 minutos, según lo establecido por las normas de la compañía, para proporcionar seguridad adicional para las aplicaciones de alto riesgo.

- **Control de acceso a la aplicación y la información.**

Objetivo 6: Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación. Se deben utilizar medios de seguridad para restringir el acceso a y dentro de los sistemas de aplicación. El acceso lógico al software de la aplicación y la información se debería limitar a los

usuarios autorizados. Los sistemas de aplicación deberían cumplir con los siguientes puntos (ISO27000.es, 2005):

a) Controlar el acceso del usuario a la información y las funciones del sistema de aplicación, en concordancia con una política de control de acceso definida.
b) Proporcionar protección contra un acceso no autorizado de cualquier utilidad, software del sistema de operación y software malicioso que sea capaz de superar o pasar los controles del sistema o la aplicación.
c) No comprometer a otros sistemas con los cuales se comparten recursos de información.

a) Restricción del acceso a la información.

Control 22: El acceso de los usuarios y el personal de soporte a la información y las funciones del sistema de la aplicación se deben limitar en concordancia con la política de control de acceso definida.

b) Aislar el sistema confidencial.

Control 23: Los sistemas confidenciales deberían tener un ambiente de cómputo dedicado.

- **Computación y tele-trabajo móvil.**

Objetivo 7: Asegurar la seguridad de la información cuando se utiliza medios de computación y tele-trabajo móviles. La protección requerida se tendría que conmensurar con los riesgos que causan estas maneras de trabajo específicas. Cuando se utiliza computación móvil, se debería considerar los riesgos de trabajar en un ambiente desprotegido para aplicar la protección apropiada evitando riesgos de pérdida de la información. En el caso del tele-trabajo, la organización tendría que aplicar protección al lugar del tele-trabajo y asegurar que se establezcan los arreglos adecuados para esta forma de trabajar (ISO27000.es, 2005).

a) Computación y comunicaciones móviles.

Control 24: Se debería establecer una política y adoptar las medidas de seguridad apropiadas para protegerse contra los riesgos de utilizar medios de computación y comunicación móvil.

b) Tele-trabajo.

Control 25: Se debe desarrollar e implementar una política, planes operacionales y procedimientos para las actividades de tele-trabajo.

Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

- **Requerimientos de seguridad de los sistemas de información.**

Objetivo 1: Garantizar que la seguridad sea una parte integral de los sistemas de información. Los sistemas de información incluyen sistemas de operación, infraestructura, aplicaciones comerciales, productos de venta masiva, servicios y aplicaciones desarrolladas por el usuario. El diseño e implementación del sistema de información que soporta el proceso comercial puede ser crucial para la seguridad. Para lo cual se debe identificar y acordar los requerimientos de seguridad antes del desarrollo y/o implementación de los sistemas de información.

Se tendría que identificar todos los requerimientos de seguridad en la fase de requerimientos de un proyecto; los cuales deben ser justificados, acordados y documentados como parte del caso comercial general para un sistema de información.

a) Análisis y especificaciones de los requerimientos de seguridad.

Control 1: Los enunciados de los requerimientos comerciales para los sistemas de información nuevos, ó las mejoras a los sistemas de información existentes, deberían especificar los requerimientos de los controles de seguridad.

Los requerimientos para la seguridad de la información y los procesos para implementar la seguridad deberían ser integrados en las primeras

etapas de los proyectos de sistemas de información. Los controles introducidos en la etapa de diseño son significativamente más baratos de implementar y mantener que aquellos incluidos durante o después de la implementación

- **Procesamiento correcto en las aplicaciones.**

Objetivo 2: Prevenir errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones. Se deben diseñar controles apropiados en las aplicaciones, incluyendo las aplicaciones desarrolladas por el usuario para asegurar un procesamiento correcto. Estos controles tienen que incluir la validación de la input data, procesamiento interno y output data.

Se pueden requerir controles adicionales para los sistemas que procesan, ó tienen impacto sobre, la información confidencial, valiosa o crítica. Estos controles se deberían determinar sobre la base de los requerimientos de seguridad y la evaluación del riesgo.

a) Validación de la input data.

Control 2: Se debe validar la input data para las aplicaciones para asegurar que esta data sea correcta y apropiada.

b) Control de procesamiento interno.

Control 3: Los chequeos de validación se deberían incorporar en las aplicaciones para detectar cualquier corrupción de la información a través de errores de procesamiento o actos deliberados.

c) Integridad del mensaje.

Control 4: Se deben identificar los requerimientos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, y se tendría que determinar e implementar los controles apropiados (ISO27000.es, 2005).

d) Validación de la output date.

Control 5: Se debería validad la output date de una aplicación para asegurar que el procesamiento de la información almacenada sea el correcto y el apropiado para las circunstancias.

- **Controles criptográficos.**

Objetivo 3: Proteger la confidencialidad, autenticidad ó integridad a través de medios criptográficos. Se debería desarrollar una política sobre el uso de controles criptográficos, y establecer una gestión clave para sostener el uso de técnicas criptográficas, siempre y cuando estén apegadas a las normas establecidas por la compañía.

a) Validación de la output date.

Control 6: Se deberá desarrollar e implementar una política sobre el uso de controles criptográficos para proteger la información.

b) Gestión de claves.

Control 7: Se tendría que establecer la gestión de claves para dar soporte al uso de técnicas criptográficas en la organización.

- **Seguridad de los archivos del sistema.**

Objetivo 4: Garantizar la seguridad de los archivos del sistema. Para lo cual se debe controlar el acceso a los archivos del sistema y el código fuente del programa, y los proyectos TI y las actividades de soporte se deberían realizar de una manera segura.

a) Control de software operacional.

Control 8: Se debería establecer procedimientos para el control de la instalación del software en los sistemas operacionales.

b) Protección de la data del sistema.

Control 9: La data de prueba se tendría que seleccionar cuidadosamente, y se la debe proteger y controlar de manera que siempre se encuentre disponible.

c) Control de acceso al código fuente del programa.

Control 10: Se debe restringir el acceso al código fuente del programa.

- **Seguridad en los procesos de desarrollo y soporte.**

Objetivo 5: Mantener la seguridad del software y la información del sistema de aplicación. Se debe controlar estrictamente los ambientes del proyecto y soporte.

Los gerentes responsables por los sistemas de aplicación también deberían ser responsables por la seguridad del ambiente del proyecto o el soporte. Ellos deberían asegurar que todos los cambios propuestos para el sistema sean revisados para chequear que no comprometan la seguridad del sistema o el ambiente de operación.

a) Procedimientos del control del cambio.

Control 11: Se debería controlar la implementación de los cambios mediante el uso de procedimientos formales para el control de cambio.

b) Revisión técnica de la aplicación de cambios en el sistema.

Control 12: Cuando se cambian los sistemas de operación, se debe revisar y probar las aplicaciones comerciales críticas para asegurar que no exista un impacto adverso sobre las operaciones organizacionales o en la seguridad.

c) Restricciones sobre los cambios en los paquetes de software.

Control 13: No se debe fomentar modificaciones a los paquetes de software, se tendría que limitar a los cambios necesarios y todos los cambios deben ser estrictamente controlados.

d) Filtración de información.

Control 14: Se debe evitar que exista alguna oportunidad para que se produzca una filtración de información.

e) Desarrollo de software abastecido externamente.

Control 15: El desarrollo del software provisto externamente deberá ser supervisado y monitoreado por personal de la organización.

- **Gestión de la vulnerabilidad técnica.**

Objetivo 6: Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas. Se debe implementar una gestión de la vulnerabilidad técnica de una manera efectiva, sistemática y respetable, tomando mediciones para confirmar su efectividad. Estas consideraciones se deben incluir a los sistemas de operación y cualquier otra aplicación en uso.

a) Control de las vulnerabilidades técnicas.

Control 16: Se tendría que obtener oportunamente la información sobre las vulnerabilidades técnicas de los sistemas de información que se están utilizando, la exposición de la organización a dichas vulnerabilidades evaluadas y las medidas apropiadas tomadas para tratar los riesgos asociados.

Gestión de Incidentes de seguridad de la información.

- **Reporte de los eventos y debilidades de la seguridad de la información.**

Objetivo 1: Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna.

Se deberían establecer procedimientos formales de reporte y de la intensificación de un evento**.** Todos los usuarios, empleados contratistas y terceros deben estar al tanto de los procedimientos para el reporte de los diferentes tipos de eventos y debilidades que podrían tener un impacto en la seguridad de los activos organizacionales. Se les instruiría para que reporten cualquier evento y debilidad de la seguridad de la información, inmediatamente ocurrido dicho evento, al punto de contacto designado.

a) Reporte de eventos en la seguridad de la información.

Control 1: Los eventos de seguridad de la información deberán ser reportados a través de los canales gerenciales apropiados lo más rápidamente posible.

b) Reporte de las debilidades en la seguridad.

Control 2: Se debe requerir que todos los usuarios empleados, contratistas y terceros de los sistemas y servicios de la información tomen nota y reporten cualquier debilidad de seguridad observada o sospechada en el sistema o los servicios.

- **Gestión de los incidentes y mejoras en la seguridad de la información.**

Objetivo 2: Asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información. Se deben establecer las responsabilidades y procedimientos para manejar de manera efectiva los eventos y debilidades en la seguridad de la información una vez

que han sido reportados. Se debería aplicar un proceso de mejoramiento continuo para la respuesta a monitoreo, evaluación y la gestión general de los incidentes en la seguridad de la información.

Cuando se requiera evidencia, esta se tendría que recolectar cumpliendo con los requerimientos legales establecidos por las normas y reglamentos internos de la compañía.

a) Responsabilidades y procedimientos.

Control 3: Se deben establecer las responsabilidades y procedimientos de la gerencia para asegurar una respuesta rápida, efectiva y metódica ante los incidentes de la seguridad de la información.

b) Aprender de los incidentes en la seguridad de la información.

Control 4: Se deben establecer mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información.

c) Recolección de evidencia.

Control 5: Cuando una acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (ya sea civil ó criminal), se debe recolectar, mantener y presentar evidencia para cumplir con las reglas de evidencia establecidas en las jurisdicciones relevantes (ISO27000.es, 2005).

CAPITULO III
SITUACIÓN ACTUAL DE PRONACA

3.1 Historia.

A partir del año de 1957 nace un gran sueño que tiempo después se convertiría en lo que hoy es PRONACA, que con el esfuerzo, trabajo, creatividad y constancia, se ha convertido en una empresa procesadora y comercializadora de alimentos que ha alcanzado el reconocimiento por la alta calidad de sus productos que provienen de los sectores: cárnico, agroindustrial y acuacultura.

Una pequeña empresa de insumos agrícolas, un sueño de hombres visionarios, puso la semilla de la PRONACA de hoy. Hace más de 50 años, INDIA dio los primeros pasos de esta industria que ahora llega a las mesas ecuatorianas con más de 800 productos alimenticios y ofrece trabajo y bienestar a miles de familias en todo el país.

Figura 5 INDIA en sus inicios.

Los inicios fueron en la línea avícola, primero en la incubación y la producción de huevos comerciales, luego en el procesamiento y venta de pollos y pavos. Más adelante, incursionamos en la producción de alimentos balanceados, y en los noventas llegó la diversificación en productos cárnicos con la producción de cerdos y embutidos y llegaron los productos de mar para exportación y mercado interno.

Figura 6 INDAVES, planta de aves Yaruquí, planta de cerdos Santo Domingo, planta de balanceados Puembo y planta de embutidos Pifo.

Se abrieron nuevos campos en la industria alimenticia con conservas y arroz. Las necesidades del consumidor nos llevaron a desarrollar creativas y prácticas opciones en alimentos precocidos. Después, decidimos llevar lo mejor del Ecuador al mundo, con la exportación de palmito y alcachofas.

El nuevo siglo impuso el reto de la internacionalización, lo cual llevó a que los modelos de producción y comercialización de palmito se extiendan a Brasil y de precocidos a Colombia.

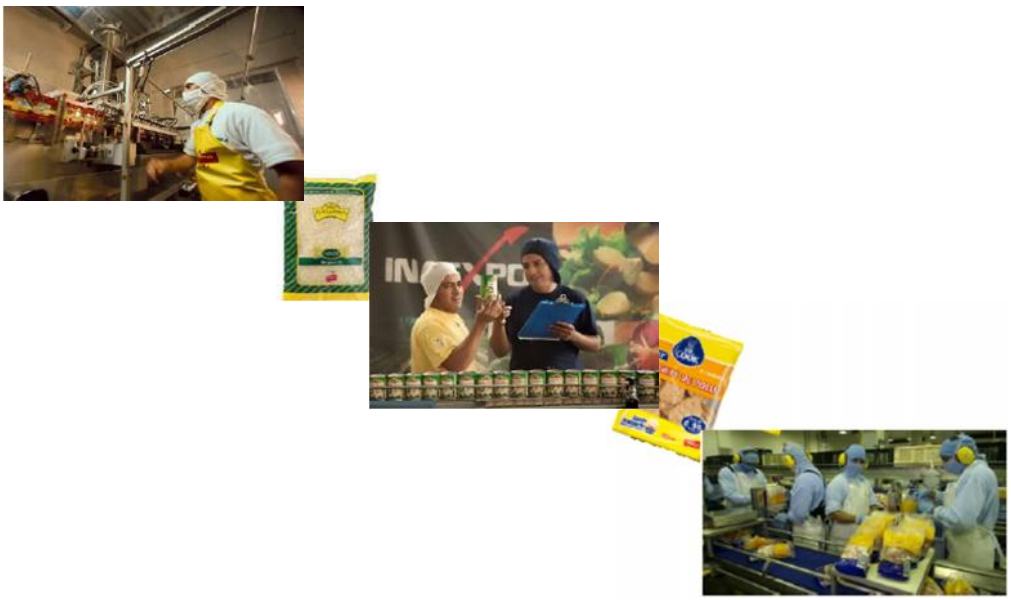

Figura 7 Planta de conservas COMANA, INAEXPO y alimentos precocidos Pifo.

Hoy, el pequeño grupo de emprendedores de hace 50 años se han transformado en una legión de miles de ecuatorianos que con trabajo y compromiso han construido esta empresa fundada sobre valores y principios invariables, distribuyendo productos a todas las familias del Ecuador.

Figura 8 Centro de Distribución Quito y Guayaquil.

3.2 Misión y Visión.

- **Misión.**

"Ser una compañía reconocida como ícono de desarrollo y fuente de trabajo. Catalogada como una empresa totalmente ecuatoriana que ofrece calidad".

- **Visión.**

"La Misión Corporativa de PRONACA, su razón de ser, establece nuestra dedicación a nuestros consumidores y al campo, cada uno de los colaboradores de PRONACA estamos aquí para alimentar bien y generar desarrollo en el sector agropecuario".

3.3 PRONACA en la actualidad.

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. Contamos con más de 7.500 colaboradores directos.

Marcas y Productos que oferta PRONACA.

PRONACA elabora y distribuye varios productos, categorizándolos en: cárnicos, secos, embutidos y alimentos balanceados para animales.

Figura 9 Marcas de PRONACA.

3.4 Organigrama de TI.

En la figura 3.6, se puede ver la estructura actual de TI con la que cuenta PRONACA.

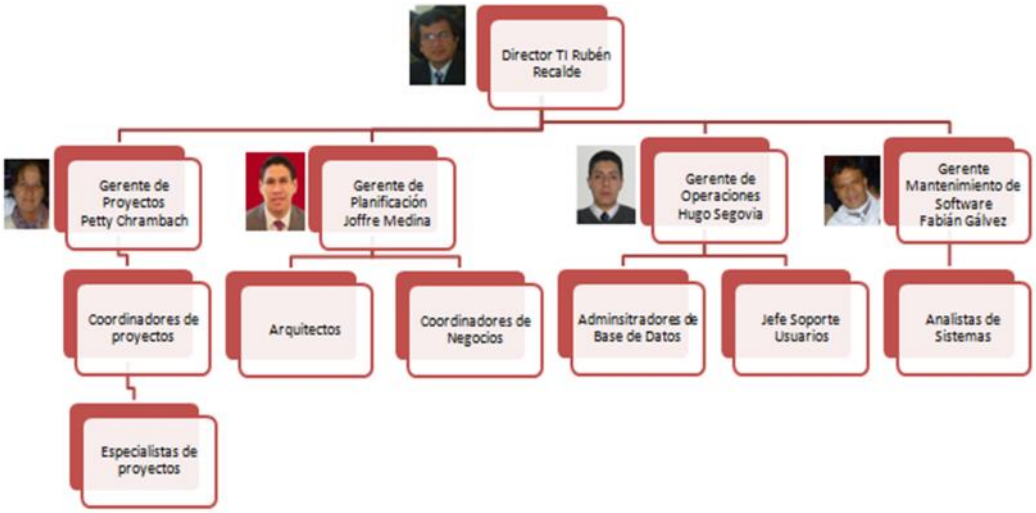

Figura 10 Dirección de TI.

3.5 Filosofía de PRONACA.

PRONACA existe para alimentar bien, generando desarrollo en el sector agropecuario.

3.6 Valores de PRONACA.

- ***INTEGRIDAD,*** en cada unos de sus actos.
- ***RESPONSABILIDAD,*** ante los clientes internos y externos.
- **SOLIDARIDAD,** con sus colaboradores y asociados.

3.7 Cadena de Valor de PRONACA.

La figura 3.7 muestra la cadena de valor bajo la cual PRONACA realiza sus actividades, es muy importante aplicar las recomendaciones de las normas ISO 27002, para la cadena de valor, ya que la información que tiene en cada uno de sus enunciados (a-k), se basan en información altamente confidencial, que debe estar segura para evitar cualquier fuga o robo de dicha información.

Figura 11 Cadena de Valor.

Toda la información de la historia, filosofía, valores, y demás temas relacionados con PRONACA, se encuentran disponibles en la intranet (http://somos:9080/pronaca/homePortalView.htm) de la compañía con acceso a todos los empleados, para de esta manera incentivar y fomentar el compromiso y amor al lugar de trabajo.

3.8 Análisis de la situación actual de la seguridad informática en PRONACA.

Se ha definido ó elegido 3 de los 11 dominios de la norma ISO 27002, para aplicar en PRONACA, debido a que estos 3 dominios se centran en la seguridad y control de acceso de la información, que es lo más importante tener controlado para la compañía en este momento, debido a situaciones de riesgo que se han presentado en estos últimos tiempos. La norma ISO 27002 menciona que se puede aplicar las recomendaciones de uno o varios dominios que el usuario elija según la importancia o necesidad que tiene la compañía a certificarse.

En la actualidad PRONACA cuenta con algunos procedimientos y políticas que se encuentran disponibles en la intranet de la compañía (http://somos:9080/pronaca/homePortalView.htm), para los empleados dependiendo del área en la que laboren, ya que debe contar con permisos de acceso, estos procedimientos se relacionan con los tres dominios que

estamos desarrollando, protección para controlar los accesos, adquisición, mantenimiento y control de las aplicaciones y medios de comunicación, que servirán como base para la implementación de las recomendaciones de la norma ISO 27002, los cuales se describen a continuación:

3.8.1 Permisos o privilegios de usuarios.

Los permisos a usuarios en PRONACA, son asignados por técnicos del área de Soporte a Usuarios, por medio de un servidor de Active Directory, los cuales podrán tener perfiles de Administrador o como un usuario con privilegios restringidos, una vez que un usuario tiene creado su perfil, este puede ingresar en cualquier computador, que este dentro del dominio de PRONACA.

Todos los técnicos Soporte a Usuarios tienen un perfil de administrador, ya que sin este perfil no pueden instalar ninguna aplicación en los computadores, además se cuenta con una clave de administrador local, para cuando es necesario sacar del dominio a un computador por daños en los perfiles, esta clave únicamente la tiene el administrador de red.

3.8.2 Password o contraseñas.

Las contraseñas son definidas por los técnicos de Soporte a Usuarios, los cuales asignan un password al momento de preparar la máquina de un usuario nuevo, el cual debe cambiar dicha clave con su primer ingreso al Microsoft Windows.

Al momento realizar el cambio de password, existe una validación del mínimo número de caracteres seis y que no se repita una clave anterior. Si al usuario se le olvida la contraseña, este deberá solicitar a técnicos de Soporte a Usuarios su cambio, para que el usuario pueda ingresar a su equipo, y de inmediato lo haga le pedirá que cambie su contraseña a una nueva.

3.8.3 Inactividad de equipos.

Cuando un usuario deja de utilizar su computador, este se bloqueará después de diez minutos, colocándose un protector de escritorio con la filosofía de PRONACA, una vez transcurridos diez minutos más, la computadora se pondrá en un estado de ahorro de energía, si por algún motivo el usuario necesita que su computador no se ponga en estado de ahorro de energía, este debe presentar la debida justificación al administrador de red para que proceda a quitarle dicha política de bloqueo. Cuando el usuario requiera nuevamente hacer uso de su equipo, deberá ingresar nuevamente su contraseña.

Todos los equipos que se usan en PRONACA tienen software con sus respectivas licencias y ningún usuario puede instalar alguna aplicación, ya que no tienen los permisos para hacerlo, de esta manera se precautela el uso de software no licenciado.

3.8.5 Uso de internet.

- **Objetivo.**

Definir las pautas generales para asegurar una adecuada protección de la información de la compañía en el uso de los servicios de Internet.

- **Alcance.**

Este procedimiento es aplicable a PRONACA y todas sus compañías relacionadas, para que sus usuarios accedan a internet de manera segura y solo a las páginas autorizadas.

- **Exposición del procedimiento.**

Todas las conexiones deben realizarse a través de un Firewall. En el caso particular de las conexiones satelitales, estas deben ser validadas a través de un servidor de tipo AAA (que verifica la autenticidad – Authentication, la autorización – Authorization y el monitoreo – Accounting de la cuenta de usuario) a fin de controlar los accesos de los usuarios, para

lo cual se debe llevar un registro de los servicios utilizados que contenga como mínimo: la cuenta de usuario, la dirección IP accedida, la dirección URL accedida, la fecha y hora.

Para el acceso al Internet es necesario tener la autorización por parte del Gerente del negocio o Director corporativo correspondiente, y será el Gerente Técnico de Tecnología y Medios quien colaborará en la configuración de las direcciones a las cuales deberá tener acceso. Es necesario aclarar que esta cuenta tiene validez hasta que haya terminado la relación laboral del usuario con PRONACA, siendo eliminada inmediatamente una vez concluida la relación.

Este servicio debe utilizarse exclusivamente para tareas propias de la función desarrollada en la compañía y no debe utilizarse para ningún otro fin.

- **Responsabilidades.**

Todos los empleados y usuarios de PROANACA y sus compañías Relacionadas.
Director Corporativo de Tecnología y Medios.

3.8.6 Acceso al Data Center.

- **Objetivo**

Establecer lineamientos generales para la definición y control de los registros de acceso al Data Center en la oficina matriz.

- **Alcance**

Aplicable 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 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 del Edificio Inverna.

El Gerente Técnico y Telecomunicaciones es la única persona que autoriza el ingreso al Data Center, a través de programación que realiza el personal de la Cabina de Seguridad de las tarjetas de acceso al personal de Tecnologías de la Información, sean estos Administradores de Base de Datos, Arquitecto de Aplicaciones o Analistas de Sistemas.

- **Responsabilidades**

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

3.8.7 Administración y control de acceso a la Información.

- **Objetivo**

Definir el proceso que asegure que todos los usuarios tengan exclusivamente el acceso a la información necesaria para el desarrollo de sus tareas habituales en la compañía.

- **Alcance**

Este procedimiento es aplicable para todos los Sistemas que son de uso de PRONACA y de sus compañías Relacionadas, siempre y cuando la tecnología lo permita, para lo cual se usarán herramientas disponibles en el mercado.

- **Exposición del procedimiento**

Creación de un usuario cuando un colaborador requiere acceso a un sistema informático, se le puede modificar los accesos cuando estos sean

requeridos. 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.

Para administrar los accesos de los usuarios, se debe cumplir con los siguientes requisitos: Solicitud de accesos por parte de nomina, autorización dependiendo de las tareas habituales que desarrollara el usuario, autenticación asignada por medio de una clave, ejecución que se la realizará por el Técnico del área de Tecnología y Medios, compromiso del usuario de responsabilidad y confidencialidad del uso de su cuenta.

- **Responsabilidades**

Directorio.
Colaboradores y usuarios.
Gerentes de Negocio y Directores.
Dirección de Desarrollo Organizacional.
Director de Tecnología y Medios.
Dirección de Auditoría y Contraloría.

3.8.8 Adquisición de bienes y servicios de Tecnología.

- **Objetivo**

Establecer lineamientos para comprar productos y/o servicios de Tecnología.

- **Alcance**

Esta política es aplicable a PRONACA y sus compañías Relacionadas.

- **Exposición del procedimiento**

El personal de Soporte a Usuarios de TI recibe los requerimientos de hardware y/o software por parte de los usuarios, valida el requerimiento y lo envía a la Gerencia de Soporte Usuarios para el trámite. Las compras de activos fijos: computadoras, servidores, switches, centrales telefónicas,

teléfonos, proyectores, impresoras, deben ser canalizados a través de la Gerencia Técnica o de la Gerencia de Soporte enviando el requerimiento por mail, se llena un formulario interno provisto por el área de compras que lo aprueba la Dirección de Tecnología y se realiza la compra a través del departamento de compras del edificio matriz.

Si existe daño en un equipo que no puede ser reparado por el personal de Soporte Usuarios, este debe ser enviado a un servicio técnico autorizado que previamente haya sido calificado como proveedor por las direcciones de Compras y Tecnología, esto se realizará solo si el equipo no está dentro de la garantía que tiene cada dispositivo.

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

- **Responsabilidades**

Dirección de compras.
Dirección de Tecnología Informática.

3.8.9 Adquisición de nuevos proyectos de tecnología.

- **Objetivo**

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

- **Alcance**

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

- **Exposición del procedimiento**

Solicitud de requerimiento de autorización de un proceso, con los objetivos planteados para luego definir la situación actual, y la descripción del nuevo requerimiento.

Revisión de la planificación y ejecución del proyecto, en donde se revisará si el proyecto no está planificado, ni presupuestado, ni consta en el plan de trabajo del año en curso, el área de Tecnología, revisará la disponibilidad de los recursos y la prioridad de los proyectos, con los costos del proyecto el área solicitante, justificará y solicitará la aprobación de un Director Corporativo ó un Gerente de Negocio, para la ejecución del mismo.

Una vez que se cuenta con la aprobación, se pasa a la definición de la herramienta y recursos del proyecto, en donde se reunirá el Gerente Técnico, Coordinador de sistemas del área, Gerente de Proyectos y/o Gerente de Soporte del área de Tecnología, para su revisión, análisis, definición de los requerimientos y el proceso de ejecución. Este nuevo Software se lo puede adquirir de varias maneras, como son:

Desarrollo interno.- con recursos propios de la organización.

Desarrollo externo.- puede ser tercerizado y /o recursos internos, según la aplicación que se requiera, la arquitectura del hardware y la herramienta en la que se desarrollará, se contacta con el proveedor de Software, el mismo que debe estar calificado como socio de negocios del grupo, con estas herramientas, se definirá la arquitectura lógica según las disposiciones del área de Tecnología.

Software comprado.- puede ser un paquete o sistema comprado, es decir ya desarrollado, con su lenguaje y arquitectura propia.

Para el desarrollo del proyecto, se conforma un grupo interno que estará a cargo durante cada paso y fase de desarrollo y/o adquisición, del Software, que son: un Líder Funcional, Usuarios Funcionales, Usuario de Control de Operaciones y/o Coordinador de Proyectos del área, un Analista Programador.

- **Responsabilidades**

Carpeta del proyecto (Contrato, Formularios, Cronogramas, Actas, Manuales) a cargo del Analista Programador interno de la organización.

Carpeta de Control de Hitos de Proyecto (Formulario de Hitos, propuestas, visión y alcance) a cargo del Gerente de Proyectos de TI.

Carpeta de Aplicaciones Data Center (Documentos de Versión y especificaciones técnicas) a cargo del Gerente de Proyectos de TI.

3.8.10 Evaluación y riesgo tecnológico.

- **Objetivo**

Definir las pautas generales para identificar y evaluar los riesgos debido al uso de tecnología, como parte del proceso global de manejo de riesgos de PRONACA y sus compañías Relacionadas.

- **Alcance**

Este procedimiento es aplicable a PRONACA y sus compañías Relacionadas, con el fin de llegar a tener una evaluación de riesgo tecnológico, que permita minimizar al máximo los posibles riesgos de seguridad que se puedan presentar.

- **Exposición del procedimiento**

La evaluación de riesgo tecnológico está dirigida hacia los recursos de información relevantes para el negocio, es decir los recursos tecnológicos

que existen para apoyar a la organización de PRONACA a alcanzar sus objetivos.

Los técnicos deberán identificar los riesgos sobre los recursos y evaluar el posible impacto en los negocios si alguno de los riesgos se materializa, además los técnicos serán los encargados de evaluar la vulnerabilidad a los riesgos, teniendo en cuenta las medidas de seguridad existentes a fin de establecer 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.

3.8.11 Seguridad de incidentes del personal.

- **Objetivo**

Minimizar el riesgo de errores humanos, amenazas, fraudes o mal uso de los Sistemas de información relevantes para PRONACA, y de igual forma asegurar que los empleados tomen conciencia de las amenazas y preocupaciones que existen sobre seguridad de la información.

- **Alcance**

Este procedimiento es aplicable a todo el personal propio o tercerizado de PRONACA y sus compañías Relacionadas, no se permitirán excepciones al presente, excepto bajo aprobación expresa y escrita del Presidente del Comité de Seguridad de la Información, quién mantendrá y retendrá la documentación de soporte durante el tiempo necesario.

- **Exposición del procedimiento**

Las responsabilidades de seguridad están incluidas en la gestión de PRONACA desde la etapa de reclutamiento de personal, la etapa de contratación y el seguimiento durante toda la vinculación laboral.

Especialmente para trabajos de alta sensibilidad, los reclutamientos potenciales de personal deben ser monitoreados en este aspecto. Todos los empleados y usuarios de procesos de información firmarán un acuerdo de confidencialidad.

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

Se requiere un entrenamiento apropiado a los colaboradores, el cual debe ser como mínimo una vez al año, y actualizaciones periódicas sobre las medidas y regulaciones de seguridad de la información.

Los procedimientos sobre incidentes cubren todo tipo de incidentes de seguridad de la información potenciales, como fallas o huecos detectados en la seguridad del sistema de información y pérdida de servicios, rechazo de servicio o incurrimiento de confidencialidad, los incidentes serán reportados a través de canales gerenciales. Todos los empleados y contratistas deben reportar cualquier incidente de seguridad a través de la comunicación a la gerencia inmediata o a cualquier miembro del Comité de Seguridad de la Información. Los usuarios no deben por si mismos tratar de eliminar cualquier infracción sospechosa, debilidad o mal funcionamiento, teniendo en cuenta que las pruebas realizadas se pueden interpretar como mal uso potencial del sistema.

Toda entrega o divulgación no autorizada de información se considerará como falta grave y aplicará la sanción prevista según reglamento interno de PRONACA. Para otros incumplimientos su gravedad será evaluada por el Comité de Seguridad de la Información a fin de aplicar la sanción correspondiente.

- **Responsabilidades**

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

Una vez definidas las políticas y procedimientos actuales en las que se basa PRONACA, es necesario realizar una reclasificación y en algunos casos la reutilización de ciertas políticas que de cierta forma hacen referencia a las recomendadas por la norma ISO 27002, mediante las cuales se presenta la propuesta del desarrollo de los tres dominios en el capítulo 4.

CAPITULO IV

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

Generalidades.

De acuerdo a los reglamentos internos que existen en PRONACA, en cada procedimiento es necesario definir el alcance y responsables de cada uno para verificar su cumplimiento y ejecución.

La información con la que cuenta PRONACA es sumamente importante, por lo cual se la debe proteger sin escatimar recursos, siendo necesaria la implementación de Políticas de Seguridad de la Información, que permitan minimizar los riesgos o daños, a los cuales se puede ver expuesta dicha información, estableciendo una cultura organizacional que permita tener el compromiso de empleados y accionistas de la organización.

Objetivo.

Proteger los recursos de Información de la compañía, ante cualquier amenaza, interna ó externa, que puedan poner en riesgo la confidencialidad, integridad, disponibilidad y confiabilidad de la información, mediante el uso de las Políticas de Seguridad de la Información, recomendadas por el estándar Internacional ISO 27002.

Alcance.

Las políticas recomendadas en este manual, se aplican a toda la compañía en los ámbitos de los tres dominios expuestos: Control del acceso, Adquisición, desarrollo y mantenimiento de de los sistemas de información y Gestión de un incidente en la seguridad de la información, con sus respectivos objetivos y controles.

Este manual tiene como finalidad proporcionar a PROANACA, directrices, procedimientos y requisitos, que permitan tener controlada su información, manteniéndola segura con políticas actualizadas de manera periódica.

Mapa conceptual de la norma ISO 27002 con los tres dominios a usar.

En la figura 4.1, podemos ver un mapa conceptual de los 3 dominios con sus respectivos objetivos de la norma ISO 27002, que son objeto de implementación para PRONACA.

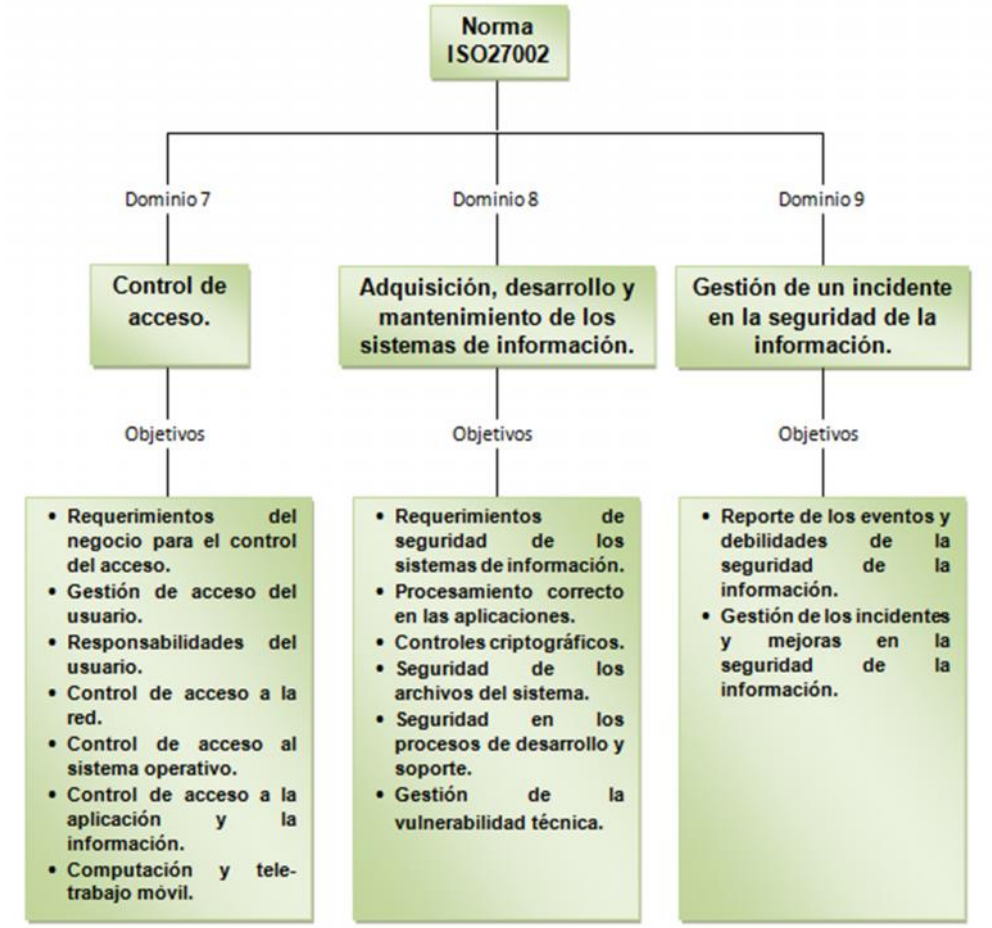

Figura 12 Mapa conceptual de los 3 dominios de la norma ISO 27002.

4.1 Control del Acceso.

4.1.1 Requerimiento del negocio para el control del acceso.

Objetivo:

Definir reglas generales que permitan controlar el acceso físico y lógico a la infraestructura, aplicaciones y sistemas con los que cuenta en la actualidad PRONACA, minimizando la probabilidad de accesos no autorizados que puedan hacer mal uso de la información.

- **Política de control de acceso.**

Es necesario determinar ciertos parámetros que nos ayuden a controlar los accesos lógicos y físicos de los usuarios.

a) Se deberán considerar los requisitos de seguridad de cada una de las aplicaciones y sistemas que son utilizados para brindar servicios a los clientes, haciendo uso y accediendo de manera exclusiva por personal con las debidas autorizaciones, que puedan garantizar la confidencialidad, integridad y disponibilidad de la información.
b) No permitir el acceso a los sistemas y aplicaciones de cuentas que no estén bien identificadas y usuarios que no dispongan de autorización de ingreso.
c) Determinar una limitación y constante monitoreo de concurrencia del uso de cuentas y usuarios con privilegios especiales, que acceden a las aplicaciones y sistemas de la compañía, como son InforLN, EAM, Trace Transport, Lotus, Outlook, entre otras.
d) Controlar el acceso de posibles usuarios impostores, por medio del bloqueo ó retardo de ingreso a las aplicaciones ó sistemas, después 3 intentos errados ó fallidos de ingreso de login y contraseña.
e) Los gerentes de cada área, serán los encargados de determinar el nivel de acceso que deberá tener cada empleado a su cargo, de acuerdo a las funciones y responsabilidades asignadas dentro de la compañía. El empleado deberá ser capacitado sobre los permisos y privilegios de acceso otorgados e incluirlos en su rol y sobre las implicaciones que

tendría el mal uso ó prestamos de sus credenciales a otros empleados. Las obligaciones deben ser incluidas en el contrato laboral desde el inicio de la presentación de sus servicios en PRONACA.

f) Se crearán perfiles estándar, los cuales estarán a cargo del departamento de control interno de PRONACA, según el puesto al que vaya a ocupar el empleado con sus funciones laborales, evitando de esta manera equivocaciones al momento de atar el empleado con un rol, esto no dependerá de una sola persona, ya que estos roles se atarán automáticamente cuando el empleado sea ingresado a la nómina de PRONACA, mediante el ADAM (Sistema Integral de Nómina y Recursos Humanos), que es el sistema de nóminas que usa la compañía. Si existe la necesidad de realizar algún cambio en los roles, se deberá anticipar con un tiempo prudencial, para evitar contratiempos en su trabajo.
g) Cuando un empleado deja de laborar en PRONACA será inactivado inmediatamente, mediante el envío de un aviso por el ADAM al sistema de Lotus, el cual envía correos a cada responsable de las diferentes aplicaciones para proceder a inactivarlo, por temas de auditoría no se lo puede borrar, además estos datos servirán a las jefaturas y direcciones para llevar un control de ingreso y salida de empleados. Se deberá revisar periódicamente los eventos y acciones que ocurren con los usuarios en cada aplicación a los que estos tienen acceso.
h) Cada jefe de Área tendrá la responsabilidad de analizar los requerimientos adicionales de accesos a otras aplicaciones ó a ciertos módulos que no estuvieron dentro del perfil de ingreso, también tendrán la potestad de retirar privilegios de ingreso si así lo estima necesario, al realizar estas acciones debe notificar al encargado de la seguridad de la Información, para su control interno.

4.1.2 Gestión de acceso del usuario.

Objetivo:

Certificar que solo los usuarios que tengan autorización puedan acceder a las aplicaciones y demás sistemas que dispone PRONACA para sus labores diarias, y además negar el acceso a usuarios no autorizados, tanto internos como externos a la compañía.

- **Registro del usuario.**

Para realizar un registro de usuario, se deberá seguir los siguientes lineamientos:

a) Estandarizar el uso de identificadores únicos para los usuarios en base a los nombres y apellidos, se formará un nombre de usuario de 8 caracteres, que contendrá la inicial del primer nombre, la inicial del segundo nombre, 5 caracteres del primer apellido y la inicial del segundo apellido, si el primer apellido tiene menos de 5 caracteres, se debe completar los 8 caracteres con las letras del segundo apellido. Para finalizar con el proceso de establecer el identificador, este debe ser documentado y entregado al usuario correspondiente.
b) Verificar que los propietarios de los accesos a las aplicaciones y sistemas de PRONACA, no hagan mal uso de los privilegios asignados, como prestar su usuario a otras personas, ya que estas terceras personas pueden realizar algún procedimiento de manera incorrecta. El incurrir con esta falta tendrá un llamado de atención a los dos usuarios, el que usa un usuario que no es el suyo, y el que presta su usuario.
c) Cuando a un usuario se le asignen permisos para trabajar en uno o varios de los sistemas y aplicaciones de PRONACA, también se le entregará un documento escrito de confidencialidad en el cual constaran las firmas de un responsable de Desarrollo Organizacional, Jefe de Tecnología y el usuario, en donde consten los derechos y deberes que tiene con las claves asignadas. Percatarse de manera precisa que el

usuario entienda el documento que está firmando, ya que el no acatar lo que en él se detalla, puede ser considerada una falta grave.

d) Se deberá llevar un registro con todos los usuarios que tienen derechos de acceso sobre los sistemas ó aplicaciones, ya que si uno de estos usuarios es removido de su cargo ó cambiado de Área, de inmediato le serán bloqueados sus permisos, para que si es el caso de cambio de Área le sean otorgados los nuevos permisos según su nuevo perfil.
e) El chequeo de los registros con los ID's de los usuarios deben ser de manera periódica, ya que de esta manera se podrán tener controlados dichos ID's para que las cuentas de los usuarios no sean redundantes, evitando tener información caducada o basura.

- **Gestión de privilegios.**

Para lograr un manejo eficaz de una gestión de privilegios, se establecerán las siguientes directrices:

a) Se deberá tener bien identificados a los usuarios con sus respectivos perfiles, para de esta manera poder asignar correctamente los privilegios que tendrá cada uno de estos usuarios a los sistemas, base de datos, y demás aplicativos con los que cuenta PRONACA según sus necesidades, para evitar riesgos en la seguridad de la información, estos privilegios serán administrados por el Jefe de cada Área conjuntamente con el encargado de la Seguridad de la Información.
b) Se realizará un procedimiento, en el cual constará a detalle la solicitud de autorización y registro de cada uno de los privilegios asignados a cada usuario, para de esta manera otorgar solo los privilegios correspondientes, sin que el usuario puede tener acceso a los sistemas y aplicativos, mientras no concluya con todos los requerimientos de dicho procedimiento.

- **Gestión de las claves secretas de los usuarios.**

Para la gestión de claves, se deberá enmarcar en los siguientes parámetros:

a) Al momento de revisar los términos del contrato laboral de ingreso a PRONACA, será un requisito el firmar un documento adjunto en el cual se haga una declaración escrita del compromiso que adquiere la persona de mantener la confidencialidad de la claves personales que se le asignen, y en caso de mantener alguna clave grupal, esta también deberá ser conocida únicamente por los miembros de dicho grupo.
b) Para que un usuario pueda tener su clave secreta, que incluso ni el Jefe de Área o el encargado de la Seguridad de la Información la conozcan, se le asignara una clave temporal segura y en el primer ingreso al sistema ó aplicación se pedirá que cambie esta clave, y de esta manera será una clave secreta que únicamente el usuario la conoce.
c) Para que una clave secreta sea aceptada por los sistemas ó aplicaciones con los que cuenta PRONACA, esta deberá tener un mínimo de 8 caracteres, entre alfabéticos, numéricos y caracteres especiales, cuando se proporcione por primera vez la clave temporal segura, esta no se la hará por mail ni por ningún otro medio que pueda ser leída por una tercera persona.
d) Será prohibido almacenar claves secretas en lugares físicos no seguros, como cuadernos, hojas, celulares, entre otros, ni en sistemas de cómputo desprotegidos.
e) Si tenemos un sistema o aplicación que ha sido adquirido externamente, el proveedor tiene la obligación de entregar las claves temporales seguras, y apenas se concluya con la instalación de dicho sistema o aplicación serán reemplazadas por claves secretas según los parámetros de la compañía.

- **Revisión de los derechos de acceso del usuario.**

La revisión de los derechos de acceso es muy importante, para lo cual se enmarcará dentro de los siguientes parámetros:

a) Los derechos de accesos de usuarios serán revisados de manera regular, cada 6 meses, ó después cualquier cambio, asenso, despido, terminación de contrato ó renuncia de un usuario de la compañía.
b) Las autorizaciones para derechos de acceso a privilegios especiales, serán revisados en intervalos frecuentes de 3 meses en donde se chequearán los privilegios asignados para asegurarse que no hayan existido cambios y que estos no estén con privilegios no autorizados.
c) Se registrará cada una de estas revisiones periódicas, para tener controlado que se realicen en las fechas establecidas y de existir algún cambio este también será registrado.

4.1.3 Responsabilidades del usuario.

Objetivo:

Definir las responsabilidades de los usuarios, para evitar el acceso de usuarios no autorizados, manteniendo fuera de peligro la información de cualquier robo, divulgación o mal uso de la misma.

- **Uso de claves secretas.**

El uso de claves secretas deberá estar sujeto a las siguientes condiciones:

a) Mantenerse bajo confidencialidad, la clave será única y estará a disposición únicamente del usuario, el cual deberá mantenerla solo para su uso y no se la debe entregar a ninguna otra persona.
b) Las contraseñas, no deberán estar escritas en papel, archivos electrónicos ó cualquier otro medio de almacenamiento no autorizado, el Encargado de la seguridad de la información será el único que podrá autorizar el almacenamiento de contraseñas de manera segura, con los métodos aprobados o definidos por las políticas de la organización.

c) Se realizarán cambios de contraseñas en un periodo fijo de 3 meses para sistemas operativos y cada 2 meses para las demás aplicaciones y sistemas que usa la compañía, en el caso que el usuario sea promovido de Área y cambie su rol ó el empleado sea separado de la organización, el cambio de contraseñas será de inmediato.

d) Al momento de establecer o definir una contraseña se debe tomar en cuenta que debe ser fácil de recordar, pero difícil de adivinar por otras personas, para lo cual no se debería hacer relación la contraseña datos del usuario como número de teléfono, dirección, nombres, fechas de nacimiento. La contraseña deberá ser de mínimo 8 caracteres y debe tener caracteres alfanuméricos y especiales, evitando así caracteres consecutivos idénticos, es decir solo números ó solo letras.

e) Las claves serán cambiadas con el primer ingreso del usuario a la aplicación ó sistema, en un lapso de máximo 48 horas, caso contrario la clave temporal caducará y deberá solicitar una nueva al administrador de la aplicación, las claves no se podrán reutilizar ó usar claves antiguas, los cual se controlará mediante validaciones en cada aplicación.

f) Las claves son secretas y los usuarios no podrán compartirla con terceras personas por ningún motivo, ya que si incumple con esta disposición será considerada una falta y se procederá según las políticas disciplinarias de PRONACA.

- **Equipo de usuario desatendido.**

Cada usuario será responsable de mantener su equipo con la debida protección, para lo cual seguirá los siguientes lineamientos:

a) Si el usuario deja su equipo sin su supervisión deberá dejarlo bloqueado, para evitar el acceso no autorizado de otras personas, divulgación ó robo de información, si un equipo es compartido por varios usuarios, cada uno deberá disponer de un usuario y contraseña para las aplicaciones y sistemas, cuando el usuario termine de realizar sus procesos tiene que cerrar la aplicación.

b) Los equipos estarán configurados para que después de 5 min de inactividad se bloqueen, según los procedimientos internos de PRONACA, y solo mediante la clave personal se podrá tener nuevamente acceso al entorno del equipo.
c) Los equipos de toda la compañía deberán ser apagados después de terminar con su jornada laboral, a excepción de los equipos que sirvan para que personal autorizado realice monitoreos ó brinde soporte, siempre contando con la autorización de los jefes de cada Área.

- **Política de escritorio y pantalla limpios.**

Los lineamientos que se deberían seguir para adoptar una política de escritorio y pantallas limpias, son los siguientes:

a) Toda información como bases de datos y respaldos de las aplicaciones que se encuentren en papel, cintas ó en algún otro tipo de medio electrónico, debe ser guardada en un lugar totalmente seguro a la cual no puedan tener acceso más que el personal autorizado, para complementar este control se definirá una política de bloqueo de sesiones inactivas cuando un equipo se encuentre sin el usuario a cargo.
b) Cuando estén sin uso terminales de trabajo, como computadores, impresoras, escáneres, fax, entre otros, estos deben quedar bloqueados y se los debe activar únicamente con claves secretas u otros medios de seguridad, además se debe proteger los puntos de ingreso y salida de correo para evitar la fuga de información, la reproducción de información es también una forma de vulnerabilidad, por este motivo las fotocopiadoras, cámaras digitales, celulares, memory flash, no se podrán usar sin su respectiva autorización de la persona encargada de la seguridad de la información, ya que se encuentran bloqueados los puertos USB de los computadores de los usuarios; además es importante mencionar que si es necesario imprimir documentos desde cualquier computador del usuario, estas impresiones no estarán disponibles, mientras que el usuario que envío a imprimir se acerque a

la impresora y digite su contraseña para que el documento se imprima, con esto se evita que personas ajenas a esta información puedan leerla ó incluso tomarla sin autorización.

4.1.4 Control de acceso a la red.

Objetivo:

Controlar el acceso a los sistemas, aplicaciones y demás servicios con los que cuenta PRONACA, tanto internos como externos, evitando de esta manera el acceso no autorizado.

- **Política sobre el uso de los servicios de la red.**

Para garantizar de alguna manera que los usuarios puedan acceder únicamente a los servicios a los que están autorizados, se deben seguir los siguientes lineamientos:

a) Los jefes o encargados de cada Área de PRONACA, juntamente con personal de Sistemas, serán los responsables de analizar las redes y servicios a las cuales determinado usuario tendrá acceso. Una vez concluidos los análisis deberán presentar un informe y solicitud al Director del departamento de TI, para que se ejecute la asignación correspondiente.
b) Para cada acceso a la red, se utilizarán medios de control y procedimientos, que permitirán llevar una estadística diaria de todos los accesos a la red que se han producido. Además solo se usarán medios de acceso permitidos por las políticas de la compañía y bajo ningún concepto se admitirá lo contrario.

- **Autenticación del usuario para las conexiones externas.**

a) Para garantizar la seguridad, al momento que usuarios con los debidos permisos puedan acceder a la red de PRONACA a través de un acceso externo, para realizar tareas específicas de soporte, se ha definido la política de acceso vía red privada virtual ó VPN, la cual estará configurada por usuario, es decir se debe asignar permisos a dicho

usuario y colocado en el respectivo grupo, para que quede habilitado y pueda acceder de forma segura.

b) Cada jefe de Área será el responsable de solicitar el acceso remoto para sus empleados, los cuales serán capacitados y debidamente entrenados para evitar riesgos y de esta manera precautelar la seguridad de la compañía.

- **Identificación del equipo en las redes.**

a) Con el propósito de tener una autenticación de las conexiones desde los equipos de PRONACA, y de las ubicaciones específicas de los mismos, se identificarán dichos equipos que formen parte de las redes informáticas de la compañía, con planos de ubicaciones a nivel nacional.

b) En la configuración lógica de cada equipo se procederá a nombrar de tal manera que se usará un estándar que permita identificar con claridad de que equipo se trata, la ubicación e importancia.

c) Para la identificación física, cada equipo será etiquetado, en la cual constará información relevante sobre las redes a las cuales puede ser conectado, con las respectivas indicaciones si tiene alguna sensibilidad ó alguna restricción.

- **Protección del puerto de diagnóstico y configuración remoto.**

a) Es muy importante la protección de los puertos de configuración y diagnóstico remoto, para lo cual se utilizarán las cuentas asignadas con sus debidas contraseñas que han sido proporcionadas únicamente al personal autorizado.

b) Todos los puertos que pueden ser causa de ingresos no autorizados de personas externas, deben ser cerrados ó inhabitados, y se los abrirá si fuere necesario, pero con el respectivo control y bajo un exhaustivo y continuo monitoreo del ó los puertos abiertos ó habilitados. Inmediatamente después de terminar su uso, se los debe deshabilitar.

- **Segregación en redes.**

a) Se deberá separar los entornos de seguridad de la red; para lo cual es necesario separarla en dominios, uno para la red interna y otro para la externa, los accesos a estos dominios debe ser por medio de un usuario y contraseña, de esta manera evitamos poner en riesgo la información que está dentro del dominio interno, que es en donde está toda la operación de PRONACA.
b) Las redes inalámbricas de igual manera serán controladas por las políticas de acceso que tiene establecidas PRONACA, para los usuarios internos y externos que estén de visita en la compañía, a estas redes solo podrán acceder mediante una solicitud al jefe de Soporte a Usuarios, y será por tiempo limitado dependiendo de la necesidad del usuario.
c) Se deberá configurar entornos totalmente aislados, los cuales podrán servir para realizar pruebas sin que ponga en riesgo la operatividad de la compañía.

- **Control de conexión a la red.**

a) Se debe cumplir de manera estricta las políticas de acceso por parte de los proveedores a las aplicaciones y sistemas de la compañía, los cuales acceden para brindar soporte, se debe monitorear de manera constante mientras el proveedor permanece conectado y además con la supervisión de un usuario funcional quien será el encargado de revisar paso a paso lo que el proveedor está realizando en la aplicación, el proveedor solo podrá acceder a la red únicamente los días laborables, entre Lunes y Viernes, mientras que los fines de semana será bloqueado su acceso, para evitar riesgos en la seguridad de la información de la compañía, si es necesario acceso de un proveedor el fin de semana, únicamente se lo hará con la debida autorización del gerente de Operaciones y del gerente de Mantenimiento de Software.
b) Las interfaces externas al sistema principal de la compañía como lo son mensajería, transferencia de archivos, entre otros, lo hará con un

usuario genérico, el cual estará a cargo del jefe del Área y este deberá certificar que dicho usuario genérico es solo de interfaz y no de uso regular.

- **Control de routing de la red.**

a) El routing ó enrutamiento correcto de la red de PRONACA, se encuentra controlado, por protocolos de capa 3, los cuales nos proporcionan un nivel muy confiable, ya que podemos verificar las direcciones fuentes y destino, además de generar alertas en caso de detectar errores en el envío y recepción de información, minimizando de esta manera las amenazas de ataques o riesgos.
b) En nivel de seguridad para el intercambio de información entre PRONACA y los distribuidores zonales, tiene mayores controles y constantes monitoreos, por el riesgo que puede existir de ataques por medio de estos canales, ya que la comunicación es diaria y durante las 24 horas del día.

4.1.5 Control del acceso al sistema operativo.

Objetivo:

Evitar que usuarios no autorizados tengan acceso a los Sistemas Operativos con los cuales trabaja la compañía.

- **Procedimientos para un registro seguro.**

Es importante controlar el inicio de a un Sistema Operativo, para lo cual se deben seguir los siguientes lineamientos:

a) Cuando se registra por primera vez un usuario, el sistema no mostrará información que sea innecesaria, ya que esta se puede usar de manera incorrecta por una tercera persona, perjudicando la confidencialidad de la compañía.

b) Lo único que se mostrará serán mensajes de advertencia generales, es decir simplemente le indicará que el usuario es un usuario no autorizado.
c) Después de 3 intentos de registro infructuoso, el sistema se bloqueará, registrando estos 3 intentos fallidos, forzando al sistema que no le permita registrarse por un lapso de 2 horas, según los procedimientos internos de PRONACA.
d) Cuando un registro es exitoso mostrará como información para el usuario la fecha y hora del registro, con detalles de su registro y advertencias sobre las contraseñas, para que las cambie si son temporales y tenga en sitios seguros.
e) Las contraseñas se escribirán en los sistemas de manera escondida mediante símbolos, para evitar que terceras personas puedan obtenerla, además las contraseñas no podrán ser transmitidas en texto ó por red.

- **Identificación y autenticación del usuario.**

a) Cada usuario tendrá asignado un identificador de usuario ó ID con su respectiva contraseña, para que pueda acceder tanto lógica como física a los sistemas y aplicaciones a los cuales tiene acceso. Los jefes de cada Área serán los responsables de controlar su personal a cargo monitoreando sus actividades.
b) Para ingresar de manera física al cuarto de servidores ó data center, los usuarios con este tipo de acceso lo harán mediante la activación de autorización en su tarjeta de identificación, mediante la cual se podrá llevar un registro de ingresos y salidas, además que el usuario que ingreso tiene la obligatoriedad de especificar el motivo por el cual ingresó y que actividades realizó en el data center.

- **Sistemas de gestión de claves secretas.**

a) Los sistemas deben proporcionar la alternativa de cambiar de contraseña, cuando el usuario lo requiera, pero el sistema estará

configurado de manera que no permita establecer una contraseña que no cumpla con los requisitos de seguridad que son: mínimo 8 caracteres y esta debe tener números y letras para que tenga mayor complejidad, advirtiendo ó describiendo de esta manera estos requisitos e indicando que la contraseña ingresada no cumple con las condiciones, para que el usuario ingrese otra.

b) Evitar la reutilización de claves anteriores, para lo cual el sistema tendrá un registro de contraseñas con el cual se validará para que el sistema no acepte una contraseña que ya fue usada, además cada tres meses el sistema invalidará automáticamente la contraseña y le pedirá que el usuario la cambie.
c) Por ningún motivo las contraseñas deberán ser guardadas ó almacenadas en ningún lugar, para evitar que se produzcan serios riesgos en la seguridad de la información por robo de contraseñas y por ende por accesos no autorizados.

- **Uso de las utilidades del sistema.**

Para tener acceso a las diferentes utilidades y bondades que un sistema ó aplicación pueda brindar, es necesario enmarcarse en las siguientes directrices:

a) Establecer un procedimiento de autentificación y autorización de usuarios, mediante su ID, para tener el control de los ingresos, ya que serán limitados y tendrán un número máximo permito de usuarios ingresados.
b) Cualquier utilidad que sea usada, deberá quedar registrada, ya que dicho registro servirá para controlar los niveles de acceso autorizados a las diferentes utilidades de los sistemas, además verificar que estén siendo usadas por los usuarios adecuados de manera correcta.
c) Si existen utilidades ó software del sistema que no estén siendo usados ó que sean innecesarias, se las retirará, para evitar cualquier

vulnerabilidad que pueda desencadenar en una seria amenaza, a las operaciones de la compañía.

- **Cierre de una sesión por inactividad.**

a) Cuando una sesión no está siendo utilizada por el usuario, se vuelve muy crítica, ya que puede ser fácilmente controlada por una tercera persona ó por error involuntario se puede llegar a enviar a ejecutar procesos incorrectos, es por este motivo que siempre que se deje de usar una sesión se la debe cerrar.
b) En caso de accesos remotos a servidores de aplicación y que se los deje de usar, se debe salir de dicho acceso mediante un logoff a la sesión, para que el usuario no se quede colgado en el sistema operativo del servidor.
c) Si el usuario deja una sesión inactiva, que sobrepase los tres minutos, que es el tiempo establecido por política interna de la compañía, las sesiones se bloquearán de manera automática y solo se habilitará con un ID y contraseña de un usuario.

- **Limitación de tiempo de conexión.**

a) Para los sistemas y aplicaciones de la compañía que sean consideradas de alto riesgo, se limitará el tiempo de conexión para precautelar la seguridad de la información y evitar cualquier tipo de riesgo.
b) Se restringirá los tiempos de conexión únicamente a las horas laborales de Lunes a Viernes, a menos que exista un pedido con anticipación por parte del jefe de Área para extender estos tiempos, con absoluta responsabilidad del solicitante.
c) En algunos sistemas existirá una re-autenticación en intervalos de una hora, mientras que en otras aplicaciones simplemente se usará el bloqueo por inactividad por tiempo de uso.

4.1.6 Control de acceso a la aplicación y la información.

Objetivo:

Evitar que usuarios no autorizados puedan acceder a los sistemas de aplicación y a la información de la compañía.

- **Restricción del acceso a la información.**

a) Para restringir el acceso a la información, nos basaremos en las políticas internas establecidas de control de acceso según los perfiles de cada usuario, mientras que para controlar el acceso a las funciones del sistema de aplicación, se proporcionará una lista de menús a los usuarios, de manera que puedan acceder a la utilidad correcta sin equivocaciones.
b) Se controlará los permisos de acceso a cada usuario, dependiendo del perfil podrán leer, escribir, eliminar ó ejecutar la información, para las utilidades se controlaran los derechos de acceso.
c) Los logs generados por los sistemas de aplicación, deben ser manejadas de manera adecuada y controlada, enviado únicamente a los terminales correspondientes, estos logs, deberán ser revisados periódicamente para evitar que exista información redundante.

- **Aislar el sistema confidencial.**

a) Para aislar un sistema sensible en un entorno dedicado, el propietario de cada sistema deberá evaluar, identificar y documentar de manera explícita la sensibilidad, confidencialidad y los riesgos por los cuales se podría ver afectada la aplicación.
b) Para que se ejecuten procesos en estos sistemas aislados deben compartir recursos sólo con sistemas de aplicaciones confiables.
c) Para el aislamiento físico se contará con medios magnéticos y biométricos de acceso, para que no pueda ingresar personal no autorizado a dicho lugar.

4.2 Adquisición, desarrollo y mantenimiento de los sistemas de información.

4.2.1 Requerimientos de seguridad de los sistemas de información.

Objetivo:

Garantizar que la seguridad sea una parte integral de los sistemas de información en la compañía.

- **Análisis y especificaciones de los requerimientos de seguridad.**

Se debe especificar los siguientes requerimientos de seguridad:

a) El encargado de la Seguridad de la Información de la compañía, juntamente con el Director de TI, serán los encargados de analizar, supervisar y monitorear la implementación de los controles necesarios para que puedan garantizar la seguridad de los sistemas de información.
b) Se deben establecer directrices y políticas de uso con las debidas autorizaciones de hardware y software, para evitar el uso sin control de estos dispositivos y aplicaciones, minimizando los riesgos en la entrega normal de los servicios.
c) Se debe contar con personal preparado acerca de Seguridad de la información, que sean capaces de identificar y controlar posibles amenazas que se puedan presentar, garantizando de esta manera la confiabilidad y disponibilidad de dicha información, para conseguir esto se deben basar en revisiones periódicas de cada evento suscitado.
d) Se debe tomar en cuenta que al interactuar con entidades y sistemas externos como proveedores de servicios, se vuelve imprescindible detectar las posibles amenazas, para tenerlas controladas de manera que no signifique un riesgo para las operaciones de la compañía.
e) Si se detecta un mal manejo de una aplicación o sistema, es necesario aislarla de inmediato ya que puede producir serios daños en la información.

f) Antes de adquirir un producto, se debe tener mínimo tres propuestas de diferentes proveedores, y analizarlas detenidamente para optar por la que cumpla con todos los requerimientos de seguridad, este análisis se lo hará en conjunto con el encargado de la Seguridad y el gerente de cada Área para la cual se va adquirir dicho producto, después del respectivo análisis se debe realizar un proceso de prueba y adquisición formal con el proveedor.
g) Considerar la correcta funcionalidad de la aplicación, en sus fases de introducción y controles asociados como actualizaciones y periodo de licenciamiento, antes de adquirir el producto.
h) Los contratos serán revisados por el departamento de Legal de la compañía junto con el encargado de la Seguridad de la Información, en donde deben constar los controles que garanticen la seguridad de la información.

4.2.2 Procesamiento correcto en las aplicaciones.

Objetivo:

Prevenir posibles errores, pérdidas, modificaciones no autorizadas ó mal uso de la información en las aplicaciones, que perjudiquen las operaciones de la compañía.

- **Valoración de la input data ó datos de entrada.**

Para tener la seguridad que todo dato que se ingrese sea correcto se realizarán las siguientes verificaciones:

a) Se realizarán verificaciones de entradas duales, por medio de herramientas que nos permitan tener un control de todos los usuarios de la compañía, además estas herramientas deben ser configurables para realizar un monitoreo con sus respectivas estadísticas de los datos que ingresan, los cuales tengan valores fuera de rango, caracteres inválidos con las cuales se llena los campos de las tablas temporales cuando se trata de sistemas externos, y de tablas propias del sistema, que no excedan los límites superiores e inferiores de la data, además se

realizaran verificaciones periódicas de anchos de banda que se encuentren establecidos en los contratos con los proveedores.

b) El encargado de la Seguridad de la Información, debe ser provisto de una herramienta configurable que le envíe alertas al correo electrónico cuando existan diferencias entre los patrones ingresados en dicha herramienta y los datos registrados como los contenidos de los campos claves, archivos de datos, para confirmar que no caduquen y que la integridad de la información este intacta.
c) Cada sistema ó aplicación con los que cuenta la compañía, que en su gran parte son adquiridos a empresas de desarrollo de software y patner's exclusivos, deben tener incorporadas alertas que envíe al usuario, cuando detecte que existen caracteres inválidos, datos incompletos, que puedan dañar la tabla ó dejar inconsistente la información de la misma.
d) Los responsables de cada aplicación serán quienes deban mantener su aplicación en óptimo estado, y reportar periódicamente al encargado de la Seguridad de la Información si existe algún evento inesperado, a más de llevar una bitácora de eventos que se revisara semanalmente.
e) El encargado de la Seguridad de la Información juntamente con el responsable de la aplicación y el gerente de una área específica que usa el sistema, realizarán semestralmente una prueba de credibilidad de datos, la cual consistirá en realizar un nuevo cálculo manual para verificar que el sistema los está realizando correctamente.

- **Control de procesamiento interno.**

Los encargados de cada aplicación para la validación, cambios y revisión en las aplicaciones, deben tener en cuenta los siguientes parámetros:

a) Cuando se requiera realizar acciones de agregar modificar y borrar, debe ser realizada por un Analista de Sistemas interno de PRONACA, bajo la consultoría del proveedor del sistema ó aplicación si es necesario y de esta manera corregir el inconveniente que está teniendo dicha aplicación, ya que esto puede afectar seriamente el

funcionamiento y ocasionar retrasos en los procesos. Antes de poner en ejecución el cambio se lo debe realizar en un servidor de pruebas destinado para estos fines, y únicamente después de certificado el cambio por el analista funcional, Analista de Sistemas, gerente de Área y encargado de la Seguridad de la Información, con las firmas respectivas en el documento de control de cambios [Anexo 1] y con el respaldo respectivo, se procede a poner en producción dicho cambio.

b) El encargado de la Seguridad de la Información debe tener muy en cuenta los procedimientos para evitar que los programas se ejecuten en un orden equivocado ó que se ejecuten después de haber detectado una falla, cada sistema estará provisto de algún tipo de aplicación que permita reversar algún cambio que se hizo y que pudo ocasionar un inconveniente en la aplicación, y de esta manera asegurar el correcto funcionamiento de los datos, además de contar con una herramienta que nos permita realizar una revisión física de disco y recuperación de información colocándola en un lugar diferente para evitar que se sobrescriba.

c) Se tendrán listados de las actualizaciones que se hacen en las tablas de los sistemas, con los datos de inicio y con los actuales, para llevar un control estadístico de la incrementación de la data, para tomar en cuenta para el mantenimiento de dicha data. Además en los listados deberán constar las ejecuciones con éxito y error y cualquier otro evento que se pueda presentar en la aplicación.

- **Integridad del mensaje.**

  Es necesario evaluar los riesgos de seguridad para determinar los casos en los que se requiera integridad del mensaje para implementar los debidos controles. Se obtendrá una integridad en los mensajes, aplicando técnicas criptográficas, protegiendo la información que sea muy sensible.

- **Validación de la output data.**

Para la validación de la output data ó datos de salida, se deberá basar en los siguientes lineamientos:

a) Cualquier usuario que maneje datos de salida, debe tener la debida aprobación ó recomendación del jefe de Área, además deberá suministrar información que sea suficiente para su entendimiento por otra persona del Área y del encargado de la Seguridad de la Información.

b) El encargado del Área en emitir estos datos de salida, debe verificar que únicamente los datos que son necesarios sean los que se envíen y de manera correcta, caso contrario deberá informar de inmediato al encargado de la Seguridad de la Información para que revise y pueda controlar cualquier anomalía que se pudo haber presentado.

c) Se debe asegurar que los enlaces de comunicación se encuentran en perfecto estado y sin intermitencias, para que sean capaces de transmitir estos datos sin pérdidas ni retrasos, además se debe verificar que el ancho de banda destinado para el efecto sea el correcto de acuerdo a los contratos por medio de un proveedor y establecidos en sus contratos.

d) Antes de poner en producción el envío de datos, estos serán puestos a prueba y se definirán a los encargados del constante monitoreo durante la duración de la salida de datos y una vez que las pruebas sean satisfactorias se podrá indicar a los clientes el modo de transmisión, cada evento de transmisión será registrada para llevar un control de éxitos y fallidos en la salida de datos, en caso de fallidos se reportará al encargado de la Seguridad de la Información.

4.2.3 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.**

Se deberán establecer las siguientes directrices, para la implementación de los controles criptográficos.

a) Cuando se usan medios criptográficos, para la protección de la información, estos deben garantizar que no se verá afectada dicha información en su correcto funcionamiento y entrega normal de la misma.
b) Los controles criptográficos se usarán ó aplicarán en los servidores web y de correo, a más de las contraseñas tanto de ingresos a las aplicaciones como a las redes de la compañía.
c) Se utilizarán controles criptográficos para el Área de Tesorería, para enviar la información de los cheques de pagos a proveedores, de esta manera se evitará cualquier alteración en la información.
d) El encargado de la Seguridad de la Información será el encargado de administrar y gestionar los controles criptográficos, tanto públicas como privadas.
e) Antes de la implementación de los controles de encriptación se deberán hacer pruebas, que avalen el correcto funcionamiento de los controles, para posteriormente ponerlos en producción, garantizando de esta manera el éxito de la encriptación de la información. El encargado de autorizar la puesta en producción será el Director de TI.
f) Cuando se trate de contenido como el monitoreo de interfaces y de virus, no se podrá aplicar controles de encriptación, ya que son eventos que necesitan ser atendidos de manera inmediata y esto retrasaría ya que se realizará un proceso previo de desencriptación, para analizar los eventos ocurridos.

- **Gestión de claves.**

a) Todas las claves criptográficas estarán protegidas contra cualquier tipo de modificación, pérdida y destrucción; además deberán ser protegidas contra la divulgación no autorizada.

b) El encargado de la Seguridad de la Información, será la única persona responsable para generar las claves encriptadas de los sistemas y aplicaciones de la compañía, además dicho encargado de la Seguridad de la Información entregará una clave encriptada, únicamente después de elaborar un documento con las respectivas firmas de aceptación de las condiciones de privacidad y confidencialidad.

c) El cambio de claves se las realizará trimestralmente, a excepción de que se presente un incidente de descubrimiento de la clave, entonces se deberán cambiar de inmediato, al igual que si un empleado sale de la compañía, también se deberá realizar el cambio de las claves de manera urgente, para evitar cualquier incidente de fallas de seguridad. Todo cambio debe ser registrado y autorizado por el encargado de la Seguridad de la Información.

d) Se deberá tener un archivo histórico con las claves que se han usado incluyendo las que ya no están siendo utilizadas en ese momento, para tener un histórico de tiempos de cambio de claves y de posibles eventos suscitados. Cuando se trata de deshabilitar una clave, se deberá primero verificar que no esté siendo usada en ninguna interfaz, y después se procederá a dejarla inactiva.

e) Es importante tener un control de auditoría de las claves, para lo cual cada seis meses se realizará una revisión interna completa de la gestión de claves, para garantizar que cada una esté siendo utilizada de manera correcta y sin ningún riesgo que afecte a la compañía.

4.2.4 Seguridad de los archivos del Sistema.

Objetivo:

Garantizar la seguridad de los archivos del sistema, evitando incidentes de riesgo.

- **Control del software operacional.**

Para garantizar la seguridad de los archivos del Sistema, se deberán seguir los siguientes lineamientos:

a) Se debe realizar actualizaciones a los sistemas operativos únicamente con el control del encargado de la Seguridad de la Información y personal con experiencia capaz de solventar cualquier eventualidad que se pudiera presentar, solo una vez que se haya hecho el análisis del impacto que esta actualización ocasionará en las aplicaciones que residen en dicho sistema operativo, se llenará un documento de control de cambios [Anexo 1] previo a la actualización.
b) El Gerente de Operaciones juntamente con el encargado de la Seguridad de la Información serán los encargados de analizar los requisitos de la actualización y definir si es aplicable ó no a la compañía, además deberán garantizar que los sistemas contengan de manera exclusiva solo códigos ejecutables debidamente aprobados y no con ningún código fuente ni compiladores, garantizado que en las actualizaciones consten las librerías y bibliotecas de igual manera actualizadas. Además, deben garantizar que se realizaron las debidas pruebas tanto funcionales como técnicas, de manera exitosa, las cuales también deben ser documentadas al igual que los detalles de configuración de cada aplicación ó sistema.
c) El Gerente de Operaciones será el encargado de establecer la estrategia de restauración al estado anterior si se presenta algún inconveniente con la actualización del sistema, las actualizaciones solo se las realizarán los días Domingos, según los procedimientos internos de PRONACA, para realizar esta actualización la compañía debe contar con una herramienta configurable que permita tener respaldos diarios de las bases de datos y de los aplicativos, entonces el respaldo que se obtenga el día Sábado, será el que sirva para restaurar si se presenta algún inconveniente durante el procesos de actualización, de esta manera no se ponen en riesgo las operaciones de la compañía.
d) Se mantendrá un registro de todas las actualizaciones del sistema, objetos, librerías, bibliotecas y demás componentes del software para llevar estadísticas de cada actualización, con datos como fecha, detalles de la actualización, componentes actualizados y motivos del cambio.

- **Protección de la data del Sistema.**

Para proteger los datos que se usarán para el desarrollo de pruebas, se basarán en las siguientes directrices:

a) Deberán usar una base de datos y aplicativo de respaldo que se encuentre cargada y configurada en un servidor diferente al de producción, con un ambiente igual al real, para que las pruebas sean eficientes y sin dar lugar a ningún error, los datos del servidor de producción no se podrán usar para realizar ninguna prueba, para de esta manera evitar cualquier contratiempo con la información de los aplicativos y sistemas de la compañía.
b) Los únicos que podrán tener acceso a las base de datos de pruebas, serán el encargado de la Seguridad de la Información y el Gerente de operaciones, los cuales harán el ingreso mediante contraseñas preestablecidas y el tiempo de acceso será limitado.
c) Si es necesario copiar la información operativa en la base de pruebas, el encargado de la información será el encargado de solicitar la autorización a través de un documento para la copia, en donde se debe especificar el motivo y razones del requerimiento, y posteriormente después de realizadas las pruebas debe registrar el evento realizado y proceder a borrar la información operativa, en un tiempo máximo de 24 horas, después de terminada la prueba.

- **Control de acceso al código fuente de los programas.**

Se debe mantener un control al acceso del código fuente de los programas, para lo cual nos basaremos en los siguientes lineamientos:

a) Se restringirá el acceso al código fuente de los programas, diseños, contenido de aplicaciones y demás fuentes que permitan realizar cambios que afecten los sistemas ó aplicaciones que usa la compañía.
b) No dejar los códigos fuentes en los sistemas ó aplicaciones, ya que estos pueden ser modificados y compilados por otra persona, y producir

afecciones en el normal funcionamiento de los procesos de la compañía.

c) Los códigos fuentes estarán únicamente en un servidor de pruebas, en donde se realizarán los desarrollos y modificaciones a dichos fuentes, y únicamente después de recibir la autorización del Gerente de Operaciones se procederá a instalar el ejecutable en el servidor de producción.
d) Debe ser registrado cada evento que se produzca tanto en el ambiente de pruebas como en el de producción, para llevar un control y además con fines auditables de los diferentes cambios que se han venido realizando en los sistemas ó aplicaciones.

4.2.5 Seguridad en los procesos de desarrollo y soporte.

Objetivo:

Mantener la seguridad del software y de la información del sistema de aplicación, controlando los ambientes del proyecto y soporte.

- **Procedimientos de control de cambios.**

Es importante que todo cambio cuente con las debidas autorizaciones y registros, para lo cual se deberán seguir las siguientes directrices:

a) El encargado de la Seguridad de la Información, deberá llenar el formulario de control de cambios [Anexo 1] en el cual constará el análisis realizado antes de los cambios que se pretenden realizar en el sistema, además deberán constar los responsables, afectaciones, fechas. Todos estos datos deberán quedar registrados como evento auditable a más del documento que quedará en custodia del Gerente de Operaciones y del encargado de la Seguridad de la Información.
b) Cualquier cambio que se vaya a hacer, únicamente se lo realizará con previa autorización y lo ejecutará la persona asignada por el Gerente de Operaciones.

c) Es considerado el software, información, archivos, entidades de base de datos y hardware como unidades que pueden ser modificadas por diversas razones, como actualizaciones ó reemplazos por averías. Cuando se trate de hardware, el encargado deberá realizar un análisis semestral para verificar si es necesario realizar algún cambio notificarlo de inmediato, estos análisis serán registrados como eventos de mantenimiento.
d) Se debe conservar las versiones anteriores, como medidas de contingencias en caso de presentarse algún inconveniente que pudiera surgir después del cambio realizado.

- **Revisión técnica de la aplicación después de cambios en el sistema.**

Para realizar las revisiones técnicas, se considerará lo siguiente:

a) El encargado de la seguridad, será el responsable de revisar que los procedimientos de integridad y control de la aplicación no se hayan puesto en peligro, garantizando el correcto funcionamiento del sistema ó aplicación.
b) El gerente de operaciones será el responsable de verificar que existan recursos económicos para efectuar dichos cambios, incluyéndolos en el presupuesto anual, con entrega hasta máximo el mes de Enero de cada año según las políticas de la empresa. Además se deberá notificar a la dirección de Tecnología de la información la necesidad de realizar cambios en las aplicaciones ó sistemas hasta el mes de Diciembre de cada año, para que estas puedan ser analizadas y presentadas oportunamente para que queden dentro de mencionado presupuesto.
c) El gerente de operaciones deberá dar la responsabilidad a una persona de su Área, para que tenga contacto con el proveedor y pueda analizar los parches enviados con un especialista funcional, y puedan ver si es viable la implementación y en qué condiciones.

- **Restricciones sobre los cambios en los paquetes de software.**

En lo posible se debe evitar el tener que modificar ó customizar un paquete de software adquirido, ya que mientras más se lo cambia, existen mayores probabilidades de riesgo en el funcionamiento de la aplicación ó sistema.

Si es estrictamente necesario realizar cambios en algún módulo de la aplicación, se lo debe hacer directamente a través del proveedor según consten en los contratos, ya que como política de la compañía siempre se hará de esta manera para evitar errores en las aplicaciones y sistemas de la compañía, ya que si los desarrolladores de la compañía lo hacen, esto puede provocar que el proveedor se desentienda de los cambios y quede la aplicación vulnerable y con riesgos de posibles fallas en su normal funcionamiento.

Se deberá mantener una copia del software originalmente como se adquirió, como medida de contingencia, y a partir de esta copia se procederá a realizar cualquier cambio en la aplicación, el cambio por más mínimo que sea, se lo debe registrar y documentar respectivamente.

- **Filtración de información.**

Para evitar la filtración ó fuga de información es necesario basarse en los siguientes lineamientos:

a) Se debería prohibir el almacenamiento de información que tenga que ver con la prestación de servicios, en medios no autorizados sean personales ó de la compañía, que no tengan seguridad y que puedan ser objeto de pérdida ó robo, dentro ó fuera de las instalaciones de la compañía, cada empleado es responsable por el cumplimiento de esta política, y si no lo hace puede ser motivo de sanción.
b) El encargado de la Seguridad de la Información será el responsable de monitorear periódicamente las actividades del personal y de los

sistemas, para evitar que se filtre la información, para lo cual se monitorearán los accesos lógicos y físicos, el uso correcto de las contraseñas, el almacenamiento correcto de la documentación, además se mantendrá un registro actualizado de todos los eventos que se vayan presentando. EL encargado de la Seguridad de la Información solicitará un informe de auditoría una vez por mes para cumplir con el reglamento interno de la compañía, para detectar algún incidente y si lo hubiera, en la auditoría constará el nombre del usuario que realizó alguna acción de cambio sin autorización y este será sancionado según las políticas de la compañía.

- **Desarrollo de software abastecido externamente.**

El encargado de definir y elaborar un contrato es el gerente de operaciones con la asesoría del encargado de la Seguridad de la Información, en donde debe establecer claramente clausulas que permitan tener el control de los procedimientos que realiza la aplicación ó sistema contratado externamente, como son acuerdos de licenciamiento, derechos de propiedad intelectual, certificaciones de calidad y derechos de acceso a informes de auditorías periódicas.

Antes de realizar cualquier actualización se debe notificar al gerente de operaciones y al encargado de la Seguridad de la Información, para que después de realizar las pruebas y verificar los impactos que puedan producir en las operaciones de la compañía no afecten ningún proceso, lo aprobará bajo total responsabilidad del proveedor del sistema externo, con un tiempo de respuesta mínimo de reversar los cambios en caso que fuere necesario.

4.2.6 Control de la vulnerabilidad técnica.

Objetivo:

Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas de las aplicaciones que prestan servicios.

- **Control de las vulnerabilidades técnicas.**

Se deberá tener un listado con la información de las vulnerabilidades presentadas y con las medidas tomadas para corregir dichas vulnerabilidades, para identificar las vulnerabilidades se deberá seguir el siguiente proceso de gestión:

a) El encargado de la Seguridad de la Información deberá mantener siempre actualizada la lista de vulnerabilidades y además deberá realizar revisiones permanentes a dicho listado, en donde constarán la información necesaria, en caso que deba contactarse con el proveedor como, vendedor, versión, estado actual y las personas responsables de cada aplicación. Además será encargado de evaluar una vulnerabilidad si se llega a presentar, para mitigarla en el menor tiempo posible, evitando retrasos en los procesos de la compañía.
b) Si se llega a presentar una vulnerabilidad técnica, se deberá notificar en el menor tiempo posible, con un máximo de 1 hora según indican las políticas de la compañía, al gerente de operaciones y al encargado de la Seguridad de la Información, elaborando un informe sobre la mencionada vulnerabilidad y de cómo se ha actuando para lograr mitigarla. Después de controlar por completo la vulnerabilidad, el encargado de la Seguridad de la Información realizará monitoreos cada hora por el lapso de 1 semana según las políticas de la compañía para descartar cualquier anomalía que se pueda presentar durante este periodo y proceder a cerrar el caso.
c) Si la vulnerabilidad se corrige únicamente con la instalación de un parche, el gerente de operaciones junto con el encargado de la Seguridad de la información y el responsable de la aplicación, deberán realizar las debidas pruebas antes de instalar dicho parche, sino existe ningún parche disponible ó el tiempo de desarrollo es superior a 1 día, los procedimientos internos indican que se deberá tomar otras medidas de seguridad como aislar los servidores en donde se presento la

vulnerabilidad ó intensificar controles de seguridad y monitoreo, mientras duran los eventos de riesgo.

d) Cada uno de los eventos que se realicen, deberán ser documentados y registrados con fechas y horas de manera que siempre estén disponibles a futuro.

4.3 Gestión de un incidente en la seguridad de la información.

4.3.1 Reporte de los eventos y debilidades de la seguridad de la información.

Objetivo

Asegurar que los eventos de seguridad asociados con los sistemas de información, que se puedan presentar sean comunicados de manera inmediata con un máximo de 4 horas, según lo establecen las políticas internas de la compañía.

- **Reporte de eventos en la seguridad de la información.**

a) El gerente de operaciones en conjunto con su equipo de trabajo serán los responsables de revisar, monitorear y alertar sobre cualquier evento de seguridad que se pueda presentar, en cada una de las aplicaciones que tienen a cargo. Se puede considerar como eventos de seguridad la pérdida del servicio, mal funcionamiento de los sistemas, errores cometidos por usuarios voluntaria ó involuntariamente. Si se presenta cualquier evento de seguridad se debe registrarlo y notificar de inmediato al gerente de operaciones, para que conjuntamente con el encargado de la Seguridad de la Información se tomen las medidas apropiadas como son la mitigación directa del evento de seguridad por el usuario que la detecto ó si fuera el caso llamar al proveedor para controlarlo según constan las clausulas de los contratos firmados en el inicio de la adquisición de la aplicación ó programa.

b) Cada evento de seguridad que se presente debe ser documentado y reportado al encargado de la Seguridad de la Información, a más de registrarlo con datos como: responsable, fecha, hora, detalles del

incidente y la solución. El encargado de la seguridad de la información deberá confirmar que el evento haya sido solventado y que no ocasionó ningún otro peligro en los demás sistemas de la compañía.

- **Reporte de las debilidades en la seguridad.**

En el caso que alguno de los miembros del equipo de trabajo del Área de Operaciones, detecte ó sospeche de un posible evento de debilidad de seguridad de la información, lo debe reportar al gerente de operaciones para mitigarlo inmediatamente. Si se trata de un incidente con responsabilidad del proveedor, este debe ser reportado inmediatamente por el gerente de operaciones ó por el encargado de la Seguridad de la Información, exigiendo una solución en el menor tiempo posible y pedir que emita un reporte continúo tanto de los avances de tratamiento de la solución, como del porque se presento el evento.

4.3.2 Gestión de los incidentes y mejoras en la seguridad de la información.

Objetivo

Asegurar el uso adecuado de una gestión que se pueda aplicar de manera consistente y efectiva para el tratamiento de los incidentes de seguridad de la información.

- **Responsabilidades y procedimientos.**

a) El gerente de operaciones juntamente con el encargado de la Seguridad de la Información, serán los responsables de establecer los procedimientos que asegure una respuesta rápida, efectiva y metodológica a seguir, ante cualquier incidente de la información que se pueda presentar.
b) Los responsables del tratamiento del incidente deberán realizar un análisis e identificación de la acción correctiva y documentarlo, para que el gerente de operaciones y el encargado de la Seguridad de la Información, puedan verificar que el incidente haya sido solventado y

garantizar que se han tomado las medidas correctas para evitar reincidencias. Estos reportes deberán ser archivados digitalmente en un servidor denominado servidor de incidencias, el cual estará ubicado en el Data Center de la compañía, ya que estos reportes pueden ayudar para tratamientos de futuros incidentes.

c) Estos procesos los deberán realizar únicamente personal autorizado, los cuales tengan acceso a los sistemas y a las bases de datos.

- **Aprender de los incidentes en la seguridad de la información.**

Se deberá utilizar la información de los incidentes de la seguridad ocurridos, para llevar una estadística de los más frecuentes y de esta manera poder colocar controles adicionales que puedan ayudar para limitar la frecuencia, daño y costo en la mitigación de estos incidentes, y si es necesario revisar las políticas de seguridad, para conseguir su eficiencia y eficacia.

- **Recolección de evidencia.**

a) En los contratos laborales se deberá incluir una clausula en la cual se indique que el jefe de cada Área podrá presentar las evidencias como testimonios de compañeros, filmaciones con las cámaras de seguridad y un análisis forense del computador con el cual desempeña sus actividades diarias, las cuales tendrán validez para determinar una sanción según las políticas del procedimiento disciplinario de la compañía.

b) El departamento Legal con los abogados de la compañía será los encargados de desarrollar parámetros de defensa ó demanda con las evidencias obtenidas de un determinado evento, de modo que dicha evidencia pueda ser usada en caso que se requiera para acciones legales.

c) La evidencia documentada como archivo, copias, fotos, entre otras, quedará en custodia del encargado de la Seguridad de la Información y del gerente de operaciones en un lugar seguro a donde solo ellos

tengan acceso, mientras que si se trata de evidencia de medios de cómputo como, discos duros, memorias, etc. serán duplicados.

d) Cualquier trabajo forense que se vaya a realizar se lo debe hacer en las copias que se sacaron y no en el original, para de esta manera proteger la integridad de todo el material de evidencia. El copiado ó duplicado de la evidencia se lo debe hacer en presencia del gerente de operaciones, el Gerente de Tecnología de la Información, el encargado de la Seguridad de la Información y un representante del departamento involucrado en el incidente ocurrido.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES.

5.1 Conclusiones.

- Establecer una correcta gestión de seguridad de la información en PRONACA es fundamental, ya que la información se ha convertido en un activo sumamente importante, que debe ser cuidado minuciosamente y estar disponible, confiable y seguro en cualquier momento que se lo requiera, para lo cual se han seguido las recomendaciones de las normas internacionales ISO 27001 e ISO 27002.
- Se han determinado y revisado las políticas y normas actuales con las que cuenta PRONACA para la seguridad de su información, para tomar como punto de partida y así diseñar la propuesta de las políticas para un SGSI, que se las debe implementar en la compañía.
- El diseño para un SGSI para PRONACA, se lo ha descrito y especificado en este proyecto desde su inicio, hasta finalizar con la propuesta definitiva que se ha presentado al director de TI, para que a su vez lo pueda exponer ante el directorio de la compañía y se pueda definir la manera de su implementación en cada uno de los centros y plantas que dispone dicha compañía.
- Se ha diseñado un Sistema de Gestión de Seguridad de la Información, con tres de los dominios de la norma ISO 27002, para minimizar al máximo, los riesgos que se puedan presentar en la seguridad de la información de PRONACA, para lo cual iniciamos determinado la situación actual, para describir un proceso específico que se implementará con la aprobación del directorio de la compañía.
- Es imprescindible que el Director de TI conjuntamente con los gerentes de sistemas, definan cada uno de los recursos tecnológicos con los que cuenta la compañía y de igual manera nombren a una persona como responsable de la Seguridad de la Información, para evitar riesgos que pueden afectar la correcta operatividad de los procesos de la organización.

- Con el desarrollo de la propuesta expuesta en el presente documento se logrará mantener confiable, disponible y segura la información de la Procesadora Nacional de Alimentos, obteniendo altos niveles de seguridad con recomendaciones de estándares internacionales como lo son las normas ISO 27001 e ISO 27002.

5.2 Recomendaciones.

- Se recomienda considerar y tomar en cuenta que existen nuevas amenazas que cada día van surgiendo que pueden poner en riesgo a la seguridad de la información de la organización, por este motivo se debe realizar análisis periódicos de posibles ataques a la información.
- Es recomendable no esperar a que se produzca un ataque a la seguridad de la información, para tomar medidas correctivas, sino que en lo posible ser proactivos y adoptar acciones preventivas que puedan evitar que los riesgos se transformen en problemas que afecten la operatividad de la compañía.
- Es importante tener documentados los procedimientos operativos, en donde se detallen las tareas de mantenimiento previstas para cada mes, además se debe documentar toda incidencia que se pueda presentar, para tener un historial de incidencias, ya que nos puede ayudar para controlar en lo futuro riesgos similares.
- Se recomienda tener una área en el departamento de TI, la cual estará a cargo de la seguridad de la información, con constantes monitoreos y actualizaciones de cada tarea e incidencias presentadas, esta persona debe estar sujeta a una constante capacitación sobre Sistemas de Gestión de Seguridad de la Información.
- Antes de implementar cada control de la norma, es necesario que existan varias pruebas de funcionalidad, ya que pueden trabajar de manera diferente a lo que se esperaba y podría ocasionar que se presenten vulnerabilidades o incompatibilidades entre las aplicaciones con las que cuenta la compañía.

- La seguridad de la información de una compañía no se la debe dejar a una sola persona de TI, sino trabajar en conjunto con las diversas áreas y concientizar a todos los empleados, para que cada uno se haga responsable por cumplir a cabalidad las recomendaciones y políticas establecidas, precautelando de esta manera la información.

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.

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

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.

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