FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP, AGENCIA DORAL

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingeniero en Redes y Telecomunicaciones

Profesor Guía

Magister Carlos Marcelo Molina Colcha

Autor

Luis Fernando Molina Batallas

Año

2016

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”

Carlos Marcelo Molina Colcha

Magister en Gestión de las Comunicaciones y Tecnologías de la Información

CI: 170962421-5

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”

Luis Fernando Molina Batallas

CI: 171945203-7

AGRADECIMIENTOS

Primeramente agradezco a Dios por brindarme salud y vida y permitirme lograr alcanzar mis objetivos de vida, segundo agradezco a toda mi familia por el apoyo incondicional en el transcurso de mi carrera y por último agradezco a todos los docentes que formaron parte de mi formación profesional.

DEDICATORIA

El presente trabajo dedico a toda mi familia, a mi madre, a mi esposa, mi hermano pero de manera especial a la memoria de mi papi que está en el cielo que es el ángel y la luz que guía mi camino y a mi hermoso hijito que es la inspiración de mi vida para seguir luchando con más sacrificio y seguir adelante, a todos los amo con todo mi corazón.

RESUMEN

El actual proyecto consiste en el diseño de un sistema de gestión de seguridad de la información SGSI para la Corporación Nacional de Telecomunicaciones CNT EP en la agencia matriz Doral directamente aplicado al área del NOC, en el SGSI propuesto se elaboran políticas de seguridad conforme los requerimientos del área del NOC tomando como referencias que es un área crítica por la función desempeñada dentro de la empresa y por la información manejada internamente.

En el capítulo 1 se analiza información detallada sobre seguridad de la información incluido conceptos básicos del tema, problemas de seguridad de la información en entidades públicas nacionales, el marco legal y jurídico a nivel nacional que contemple normativas sobre seguridad de la información y se analiza la norma INEN-ISO/IEC 27001:2012 la misma que se utiliza como base y referencia para el desarrollo del diseño del SGSI propuesto.

En el capítulo 2 se analiza la situación actual de la seguridad de la información en el área del NOC, se analiza la infraestructura tecnológica utilizada en el área incluyendo el software y hardware actualmente utilizados y se analizarán los principales procesos gestionados internamente en el área con el propósito de detectar problemas relacionados a temas de seguridad de la información.

En el capítulo 3 se describirá la herramienta Alfresco como un gestor de apoyo en la gestión de documentación de información relacionados a temas de seguridad de la información tomando como referencia el esquema gubernamental de seguridad de la información que el registro oficial del actual gobierno nos brinda como guía de apoyo para el desarrollo de SGSI`s en entidades públicas a nivel nacional, adicional a esto se describen los problemas encontrados en el área del NOC y sus posibles soluciones.

En el capítulo 4 se evaluarán y detallarán los problemas detectados sobre seguridad de la información en el área del NOC, se analiza las posibles soluciones a dichos problemas aplicando o adicionando nuevas políticas propuestas según el esquema gubernamental de seguridad de la información

recomienda, se analizará las restricciones y sus posibles soluciones incluyendo análisis de factibilidad técnica y económica para estudiar una posible implementación del SGSI propuesto aclarando que la implementación del SGSI está fuera del alcance del proyecto actual.

Por último se establecerán las conclusiones y recomendaciones basándonos en todo el desarrollo del proyecto.

ABSTRACT

The current project involves the design of a management system of information security ISMS for the National Telecommunications Corporation CNT EP in the parent agency Doral directly applied to the area of the NOC, the proposed ISMS security policies are made according the requirements the area of the NOC demands and taking as references is a critical area for its role within the company and the information handled internally.

In chapter 1 detailed information is analyzed on information security including basic concepts of the topic, issues information security in national public entities, legal and legal framework at the national level that includes regulations on information security and analyzes the standard INEN-ISO/IEC 27001:2012, the same that is used as a base reference for the development and design of the proposed ISMS.

In chapter 2 the current state of information security in the area of the NOC is analyzed, the technological infrastructure used in the area including software and hardware currently used and the main processes managed will be discussed internally in the area with analyzes in order to detect problems related to issues of information security.

In chapter 3 the Alfresco tool as a manager management support documentation of information related to security issues of information by reference to the government scheme of information security that the official record of the current government gives us as described guide support for the development of SGSI`s in public institutions at national, this additional level to the problems encountered in the area of the NOC and its possible solutions.

In Chapter 4 it is assessed and detailed the problems detected on information security in the area of the NOC, possible solutions to these problems by applying or adding new policies proposed by the government scheme of information security recommended is analyzed analyze restrictions and possible solutions including analysis of technical and economic feasibility to study a

possible implementation of ISMS proposed clarifying that the implementation of the ISMS is beyond the scope of the current project.

Finally conclusions and recommendations based on the entire development of the project will be established.

ÍNDICE

INTRODUCCIÓN

Actualmente en todas las empresas públicas y privadas la información interna que se maneja es de vital importancia para el buen funcionamiento y desarrollo de las mismas; por lo que la información constituye un activo de uso delicado para dichas empresas.

Existen grandes ventajas respecto al desarrollo tecnológico que permite hacer un uso eficiente para enviar, editar, guardar o eliminar información de cualquier tipo, conforme avanza la tecnología se ofrece más recursos y facilidad para las empresas en general o los usuarios de dichas empresas para un mejor uso de la información, de igual manera también se crean nuevas formas para una mala utilización de la información o para el plagio malintencionado de la información para causar perjuicios o daños a ciertas empresas.

En nuestro caso puntual referente a la Corporación Nacional de Telecomunicaciones CNT EP se confirma que la información utilizada internamente es altamente importante y de gran confidencialidad en ciertos aspectos por lo que es necesario diseñar un Sistema de Gestión de Seguridad de la Información con el que se garantice el uso correcto de la tecnología y de las diferentes medidas de seguridad de la información.

La seguridad de la información es una forma de garantizar el buen uso de la información y brindar la seguridad que se requiera dependiendo del tipo de información que se maneje.

El propósito de este proyecto es diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) para una sucursal de la CNT EP en este caso la agencia Doral, explícitamente para el área del Centro de Operaciones de Redes NOC, las políticas contempladas en el SGSI propuesto serán diseñadas para el uso exclusivo del área y serán gestionadas internamente; la implementación, revisión, verificación y mejora de este sistema está sujeto al

criterio de la empresa mencionada y por lo tanto fuera del alcance de este proyecto.

Alcance

El presente proyecto consiste en el diseño de un sistema de gestión de seguridad de la información, el mismo que inicia con la selección de la agencia regional que servirá como caso de estudio, se realizará un análisis del estado actual de la seguridad de la información de la matriz seleccionada, tomando como referencia la norma NTE INEN-ISO/IEC 27001 se seleccionarán los procesos a ser aplicados considerando las principales necesidades identificadas anteriormente, finalmente se demostrara y evaluará la funcionalidad y viabilidad del sistema de gestión propuesto para verificar si este es adaptable al requerimiento de la empresa que es disponer de mayor seguridad en la información que la misma maneja.

Consecuentemente la implementación y la mejora del mismo está sujeto al criterio de la empresa, por lo tanto, esto está fuera del alcance del presente proyecto.

Justificación

Actualmente varias entidades públicas a nivel nacional han estado expuestas ataques graves de extracción de la información, dando como resultado serios perjuicios para las entidades. El motivo principal es la falta de políticas, normas y controles para la protección de la información vital.

Por lo tanto el presente proyecto busca diseñar un sistema de gestión de seguridad de la información, tomando en cuenta los problemas anteriormente mencionados y el estado actual de seguridad de las entidades públicas, teniendo un lineamiento base para que otras instituciones utilicen esta gestión para mejorar su seguridad institucional.

Objetivo General

Diseñar un Sistema de Gestión de Seguridad de la Información para la Corporación Nacional de Telecomunicaciones CNT EP.

Objetivos Específicos

- Describir la problemática actual de la seguridad de la información en las entidades públicas ecuatorianas.

- Analizar el estado actual de la seguridad de la información en la matriz de la Corporación Nacional de Telecomunicaciones CNT EP, Edificio Doral.

- Diseñar el sistema de gestión de seguridad de la información.

- Evaluar el sistema de gestión de seguridad de la información propuesto.

1. Capítulo I. Marco Teórico

1.1 Marco Conceptual

Existen algunos términos que se definirán a continuación para poder entender el desarrollo del proyecto.

1.2 Introducción

Los términos y definiciones que a continuación se detallarán se toman en base al requerimiento y objetivos del actual proyecto, en nuestro caso se busca diseñar un sistema de gestión de la seguridad de la información por lo que el marco teórico tiene fundamentos en base a la norma aplicada en el proyecto que es la INEN-ISO/IEC 27001:2012, esta norma detalla los fundamentos teóricos necesarios para comprender la administración de un sistema de seguridad de la información.

1.2.1 INSTITUTO ECUATORIANO DE NORMALIZACION INEN

El Instituto Ecuatoriano de Normalización, INEN, es una entidad técnica de derecho público, con personería jurídica, patrimonio y fondos propios, con autonomía administrativa, económica, financiera y operativa, siendo el organismo técnico nacional competente, en materia de reglamentación, normalización y metrología, en conformidad con lo establecido en las leyes de la república y en tratados, acuerdos y convenios internacionales.

1.2.2 Información

Para la Corporación Nacional de Telecomunicaciones CNT EP y en general para las entidades y empresas a nivel nacional la información manejada internamente es el activo más importante y de vital uso y protección para el buen funcionamiento y desarrollo de la empresa. Existen muchos conceptos aplicados al término información, para el desarrollo de nuestro proyecto la definición consecuente es que es un conjunto de datos organizados que conforman un mensaje.

1.3 Tipos de Información

Se clasifica de acuerdo al tipo de comunicación, entre ellas tenemos:

- Hablada
- Escrita
- Impresa
- Almacenada electrónicamente
- Enviada por correo electrónico o convencional
- Exhibida en videos

1.3.1 Seguridad de la Información

Es un conjunto de medidas preventivas que optan las organizaciones y grupos tecnológicos para proteger la información.

Para el desarrollo del proyecto la norma INEN-ISO/IEC 27001:2012 establece tres características fundamentales de la información para la gestión de la seguridad de la información, las mismas se detallan a continuación:

1.3.1.1 Confidencialidad

Es la accesibilidad a la información solo por parte de personal autorizado.

1.3.1.2 Disponibilidad

Es la propiedad de permitir el acceso a la información bajo el pedido de alguna persona con autorización.

1.3.1.3 Integridad

Es la forma de preservar la idoneidad de la información garantizando que esta no sea alterada o suprimida.

1.3.2 Riesgo

En nuestro caso se definiría como la probabilidad de un daño o pérdida de la información y su ocurrencia.

1.3.2.1 Administración de Riesgos

Es el proceso de identificación, análisis, evaluación y tratamiento de riesgos.

1.3.2.2 Análisis de riesgos

Es el uso de la información para estimar riesgos y su fuente de origen.

1.3.2.3 Evaluación de riesgos

Es el evento donde se comparan el riesgo con la probabilidad del riesgo para determinar la afectación del mismo.

1.3.2.4 Gestión de riesgos

Son las acciones coordinadas por una empresa según el riesgo determinado.

1.3.2.5 Tratamiento de riesgos

Son las medidas adoptadas para controlar el riesgo.

1.3.3 Control

Es la dirección u organización de un sistema.

1.3.4 Evento de la Seguridad de la Información

Es una ocurrencia que identifica una violación de las políticas o fallas en las salvaguardas del sistema de la seguridad de la información.

1.3.5 Incidente de la Seguridad de la Información

Son una serie de eventos de la seguridad de la información que representan una amenaza para la seguridad de la información.

1.3.5.1 Amenaza

Acción por la cual se puede producir un incidente que causará perjuicios a la empresa, en nuestro caso sería el mal uso, alteración o pérdidas de la información.

1.4 SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Es un conjunto de procesos de gestión de la información que ofrece principalmente un manejo efectivo de la información garantizando la accesibilidad y seguridad de la confidencialidad, integridad y disponibilidad de la información y a la vez un SGSI minimiza considerablemente los riesgos de la seguridad de la información.

1.4.1 Fundamentos

Inicialmente debemos conocer el ciclo de vida de la información y los aspectos más importantes para garantizar su confidencialidad, integridad y disponibilidad (C-I-D) (Figura 1).

Toda información procede de la siguiente manera:

1. Se crea la información.
2. Se guarda la información.
3. Se utiliza la información.
4. En ciertos casos se comparte la información.
5. En ciertos casos se archiva la información.
6. Dependiendo del caso se elimina la información.

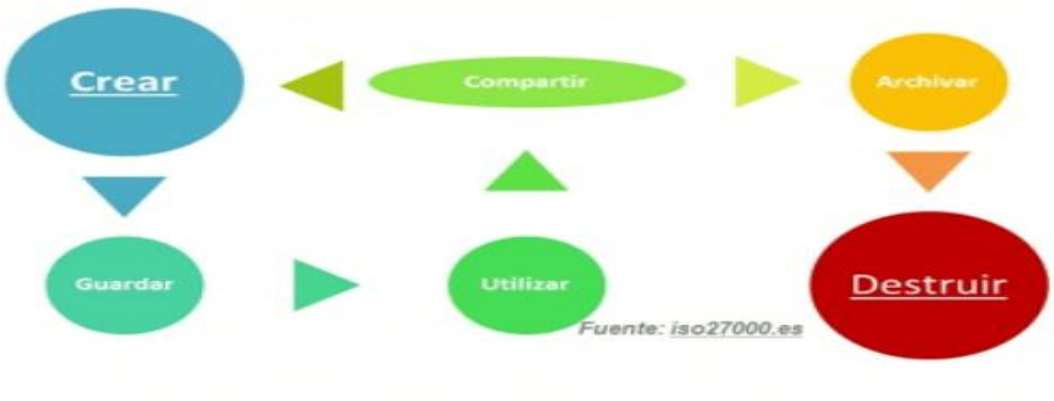


Figura 1. Ciclo de Vida de la Información
Tomado de Secretaría Nacional de la Administración Pública, s.f.

Ciertamente no se puede garantizar un nivel de protección total de la información aunque se disponga de recursos ilimitados para gestionar un SGSI. El objetivo principal de un SGSI es garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la empresa de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptable a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

1.4.2 Uso

Un activo muy importante de cada empresa es la información, procesos y sistemas que utilizan esta información, por lo tanto manejar un sistema de gestión de seguridad de la información eficiente es una forma de garantizar una buena competitividad, rentabilidad e imagen empresarial para alcanzar los objetivos empresariales.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos.

Figura 2. Proceso para Gestionar Riesgos

Tomado de Secretaría Pontificia Universidad Católica del Perú, s.f.

1.4.3 Establecimiento de un SGSI

1.4.3.1 Establecimiento

A continuación se detallan los pasos a seguir para establecer un SGSI:

1. Se define el alcance del SGSI.
2. Se define un objetivo de evaluación de riesgo.
3. Identificar los riesgos.
4. Analizar y evaluar el riesgo.
5. Identificar y evaluar las opciones para afrontar el riesgo.
6. Seleccionar objetivos de control y controles para el tratamiento de riesgos (Figura 2).

1.4.3.2 Implementación y Operación

A continuación se detallan los pasos a seguir para implementar y operar un SGSI:

1. Formular un plan de tratamiento de riesgo.
2. Revisión y aceptación del plan contra riesgos.
3. Implementar el plan de tratamiento de riesgos.
4. Manejar las operaciones del SGSI.
5. Manejar los recursos para el SGSI.
6. Implementar procedimientos y controles para la detección y respuesta a incidentes de seguridad.

1.4.3.3 Monitoreo y Revisión

A continuación se detallan los pasos a seguir para monitorear y revisar un SGSI:

1. Ejecutar procedimientos de monitoreo y ejecución.
2. Realizar revisiones regulares.
3. Medir la efectividad de los controles.
4. Revisar las evaluaciones.

1.4.3.4 Mantenimiento y Mejoramiento

A continuación se detallan los pasos a seguir para el mantener y mejorar un SGSI:

1. Implementar las mejoras identificadas.
2. Asegurar que las mejoras logren los objetivos señalados.

1.4.4 Beneficios

1. Establecer una metodología de seguridad estructurada.
2. Reducción del riesgo de pérdida, robo o corrupción de la información.
3. Se establecen medidas de seguridad para el acceso a la información.
4. Los riesgos son periódicamente revisados.
5. Garantiza operatividad de la empresa después de afrontar un problema crítico que afecte a la seguridad de la información.
6. Reducción de costos.
7. Mejora de procesos.
8. Mejora de servicios.

1.4.5 Consejos Básicos

1. Mantenerse a un alcance reducido y manejable.
2. Mantenimiento y mejora continua.

1.5 PROBLEMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN EN EMPRESAS PÚBLICAS EN EL ECUADOR

La norma INEN-ISO/IEC 27001:2012 establece una serie de políticas para una administración eficiente de la seguridad de la información en entidades públicas a nivel nacional. El objetivo de esta norma es proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) conforme las necesidades y requerimientos que la entidad establezca respecto a seguridad de la información.

Para tener una visión global del tema se realizó una encuesta en temas de seguridad de la información la cual se detallará a continuación:

1.5.1 IV Encuesta Latinoamericana de la Seguridad de la Información

Esta encuesta fue realizada en el año 2012 a diferentes líderes profesionales de tecnologías de la información, redes y telecomunicaciones, y sistemas informáticos de diversos países. En la Figura 3 se aprecia una estadística de la participación de algunos países respecto a temas de seguridad de la información.

Países Participantes	2009	2010	2011	2012
Argentina	6.50 %	12.7%	17%	23.33%
Chile	8.80%	0%	2%	2.50%
Colombia	65.04%	58.90%	60%	42.22%
Costa Rica	0%	0%	0%	7.50%
México	12.20%	10.30%	5%	5.00%
Uruguay	7.10%	6.07%	3%	1.39%
Paraguay	0%	6.38%	0%	2.80%

Países Participantes	2009	2010	2011	2012
Perú	0%	0.00%	0%	15.00%
Otros Países: Cuba, Ecuador , Panamá, Portugal Puerto Rico, Venezuela	0%	5.50%	13%	2.78%

Figura 3. Estadísticas de Participación Internacional

Tomado de Saucedo, G. y Jeimy, C., 2012.

En el año 2012 se observa una reducción considerable en la participación de nuestro país en temas referentes a seguridad de la información debido básicamente al desinterés por parte de profesionales en temáticas como la desarrollada en este proyecto.

Se puede concluir que la participación del Ecuador es reducida comparada con al resto de países lo cual ocasiona mayor probabilidad de que alguna entidad a nivel nacional sufra daños o repercusiones a un posible falla de seguridad en la

información que esta administra. Ejemplos de Casos de Fallas de Seguridad de la Información en Ecuador.

1.6 MARCO LEGAL Y JURÍDICO RESPECTO A SEGURIDAD DE LA INFORMACIÓN EN EL ECUADOR

A nivel nacional existen diversas normas y leyes respecto a seguridad de la información, a continuación se detallarán las más representativas en lo que respecta a seguridad de la información en entidades nacionales.

1.6.1 Normas de la Contraloría General del Estado

Estas normas hacen énfasis en la evaluación de riesgos y la seguridad de tecnologías de la información.

1.6.1.1 300 Evaluación de Riesgos

La máxima autoridad establecerá los mecanismos necesarios para identificar, analizar y tratar los riesgos a los que está expuesta la organización para el logro de sus objetivos.

1.6.1.2 300-01 Identificación de Riesgos

Los directivos de la entidad identificarán los riesgos que puedan afectar el logro de los objetivos institucionales debido a factores internos o externos.

1.6.1.3 300-02 Mitigación de Riesgos

Los directivos de la entidad del sector público y las personas jurídicas de derecho privado que dispongan de recursos públicos, realizarán la mitigación de riesgos desarrollando y documentando una estrategia clara.

1.6.1.4 300-03 Valoración de Riesgos

Se debe obtener la suficiente información acerca de las situaciones de riesgos para estimar su valor de ocurrencia, este análisis permite reflexionar sobre la afectación de los riesgos en los objetivos de la entidad.

1.6.1.5 300-03 Respuesta de Riesgos

Los directivos de la entidad identificarán las opciones de respuestas al riesgo, considerando la probabilidad y el impacto en relación a la tolerancia al riesgo y su relación costo/beneficio.

1.6.1.6 410-10 Seguridad de Tecnología de la Información

La Unidad de Tecnologías de la Información establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.

1.6.2 Ley de Protección a la Intimidad y a los Datos Personales

Este proyecto de ley fue propuesto por la Asamblea Nacional de la República del Ecuador con el propósito de contemplar a la Ley del Sistema Nacional de Registro de Datos Públicos y tiene por objetivo la protección al derecho a la intimidad y el tratamiento de datos personales almacenados tanto en medios físicos y digitales.

1.6.3 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

Esta ley regula el uso de sistemas de información y redes electrónicas, esta ley establece sanciones sobre infracciones informáticas cometidas por empleados públicos o personas encargadas de brindar un servicio público, la entidad reguladora de esta ley es la Contraloría General del Estado.

1.6.4 Ley del Sistema Nacional de Registro de Datos Públicos

El objetivo de esta ley es garantizar un manejo eficiente y eficaz de la información en las instituciones públicas y privadas que manejen recursos públicos. Esta ley establece algunas directrices en lo que concierne a la gestión de respaldos de la información, planes de contingencia y protección contra robos y alteraciones en la información. La entidad reguladora de esta ley es la Asamblea Nacional de la República del Ecuador.

1.6.5 Ley Orgánica de Transparencia y Acceso a la Información Pública

En esta ley se define la obligatoriedad de las instituciones públicas a proteger la información a través de normas técnicas para el manejo, archivo y documentación de la misma. La entidad reguladora de esta ley era el Congreso Nacional de la República del Ecuador.

1.6.6 Conclusión

A nivel nacional se puede concluir que las leyes y normativas creadas para solventar problemas en lo que concierne seguridad de la información carecen de fundamentos en la actualidad ya que las mismas han sido desarrolladas tomando como referencia problemáticas de años anteriores y estas normas y leyes no han sido actualizadas.

Cabe recalcar que un SGSI es un complemento que ayuda a que estas leyes se cumplan y se prosiga con un sistema organizado para que la seguridad de la información requerida por la empresa ayude a cumplir o alcanzar los objetivos de la empresa.

1.7 ESTÁNDAR INTERNACIONAL INEN-ISO/IEC 27001:2012

1.7.1 ISO 27000

Es un conjunto de estándares desarrollados por la ISO (International Organization for Standardization) y la IEC (International Electrotechnical Commission), el cual tiene por objetivo buscar un marco de gestión de la seguridad de la información que sea administrable para cualquier tipo de organización o empresa.

1.7.2 INEN-ISO/IEC 27001:2012

Es la norma principal de toda la serie 27000 en la cual se establece los requisitos para la gestión de un Sistema de Gestión de Seguridad de la Información SGSI.

A continuación se describen algunas características de la norma INEN-ISO/IEC 27001:2012:

- Sistema de gestión de la seguridad de la información: cómo crear, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI; requisitos de documentación y control de la misma.
- Responsabilidad de la dirección: en cuanto a compromiso con el SGSI, gestión y provisión de recursos y concienciación, formación y capacitación del personal.

Auditorías internas del SGSI**:** cómo realizar las auditorías internas de control y cumplimiento.

- Revisión del SGSI por la dirección**:** cómo gestionar el proceso periódico de revisión del SGSI por parte de la dirección.
- Mejora del SGSI**:** mejora continua, acciones correctivas y acciones preventivas.

1.8 COMPARACIÓN DE LA NORMA INEN-ISO/IEC 27001 CON OTRAS NORMAS EXISTENTES PARA GESTIONAR UN SGSI

Es necesario realizar una comparación entre las diferentes normas de trabajo que tienen como objetivo gestionar un sistema de gestión de la seguridad, entre estas destacaremos las características individuales y una comparación con la norma INEN-ISO/IEC 27001 la cual vamos a utilizar en nuestro proyecto.

1.8.1 AS/NZS 4360:2004

Tiene como objetivo establecer e implementar un proceso de administración de riesgos introduciendo la identificación, análisis, evaluación, tratamiento, comunicación y monitoreo de los riesgos. La administración de riesgos puede aplicarse en todos los niveles dentro de la organización.

Esta norma tiene un alto porcentaje de aceptación y utilización debido a que sus características técnicas son similares a las características de la norma INEN-ISO/IEC 27001.

1.1.1 Magerit II

Esta norma sigue los siguientes pasos para lograr una buena administración de los riesgos:

1. Reconocer los activos más importantes para la empresa.
2. Reconocer las amenazas a las que podrían estar expuestos los activos.
3. En el caso de concretarse la amenaza se debe de determinar el impacto del daño sobre el activo.
4. Costear los activos en el proceso de recuperación de la empresa después de haber sufrido un daño en el activo.
5. Determinar un valor a las amenazas más importantes.
6. Estimar el riesgo.

Esta norma busca como los objetivos más importantes:

1. Dar conocimiento a todos los que forman la empresa u organización respecto a los riesgos y el impacto que estos tendría sobre la empresa.
2. Buscar un método para mitigar los riesgos.
3. Buscar las medidas con la cuales el riesgo se lo tenga bajo control.

1.8.2 Octave

Es una metodología para la evaluación de riesgos centrándose en aquellos activos de información considerados críticos, se evalúa las amenazas hacia estos activos y se evalúa las vulnerabilidades tanto técnicas como las organizacionales de la empresa.

Esta metodología consiste en un proceso que se divide en 3 fases:

1. Construir perfiles de amenazas.
2. Identificar vulnerabilidades.
3. Desarrollar estrategias y planes de seguridad.

Para mitigar los riesgos se proporciona dos clases de prácticas:

1.8.2.1 Prácticas Operacionales

1. Seguridad física.
2. Seguridad de tecnología de la información.
3. Seguridad de personal.

1.8.2.2 Prácticas Estratégicas

1. Capacitación sobre seguridad.
2. Estrategias de seguridad.
3. Gestión de seguridad.
4. Políticas de seguridad.
5. Gestión de seguridad colaborativa.
6. Planes de contingencia.
7. Recuperación de desastres.

A diferencia de la norma INEN-ISO/IEC 27001 ésta metodología provee una serie de encuestas ya elaboradas que permiten identificar las prácticas de seguridad ya existentes en los diferentes niveles de seguridad.

1.8.3 ITIL

Esta metodología está fundamentada en las mejores prácticas de gestión de servicios de TI. Busca como objetivos entregar servicio de alta calidad al cliente, satisface las necesidades de la empresa en general o de los usuarios que la conforman y realiza revisiones periódicas y mejora de la metodología.

Como principales objetivos de la gestión tenemos:

1. Calidad en los servicios.
2. Aumentar la eficiencia.
3. Reducir los riesgos.

La diferencia con la norma INEN-ISO/IEC 27001 es que esta norma esta enfocada en la gestión de seguridad de la información y la norma ITIL esta enfocada en la gestión de servicios.

1.8.4 COBIT

Es un marco de trabajo basado en procesos enfocados en la gestión de las tecnologías de la información de una organización buscando un lineamiento de los objetivos de TI con los objetivos del negocio. Existen objetivos que COBIT establece que no necesariamente son citados por la norma INEN-ISO/IEC 27001, esto implicaría un gasto innecesario de recursos de aplicarse COBIT para la gestión de riesgos.

1.8.5 CONCLUSIÓN

Una de las principales ventajas de la norma INEN-ISO/IEC 27001 sobre las normas citadas anteriormente en la comparación de metodologías, es que la norma INEN-ISO/IEC 27001 es certificada lo que brinda mayor confianza y seguridad al utilizar esta norma para diseñar o desarrollar un sistema de gestión de la seguridad de la información y el resultado o cumplimiento de los objetivos de la empresa se alcanzarían con seguridad considerando como prioridad el buen uso de los activos y la seguridad de los mismos.

2. Capítulo II. Análisis del Estado Actual de la Seguridad de la Información en la Matriz Doral CNT

Para el análisis del sistema de seguridad de la información que actualmente se utiliza en el edificio Doral de CNT cabe destacar que este sistema se aplica por igual a todas las áreas que conforman la sucursal el Doral y se rige de acuerdo a la normas estandarizadas de seguridad de la información que las empresas públicas utilizan en Ecuador que en nuestro caso es la INEN-ISO/IEC 27001 (Anexo 1).

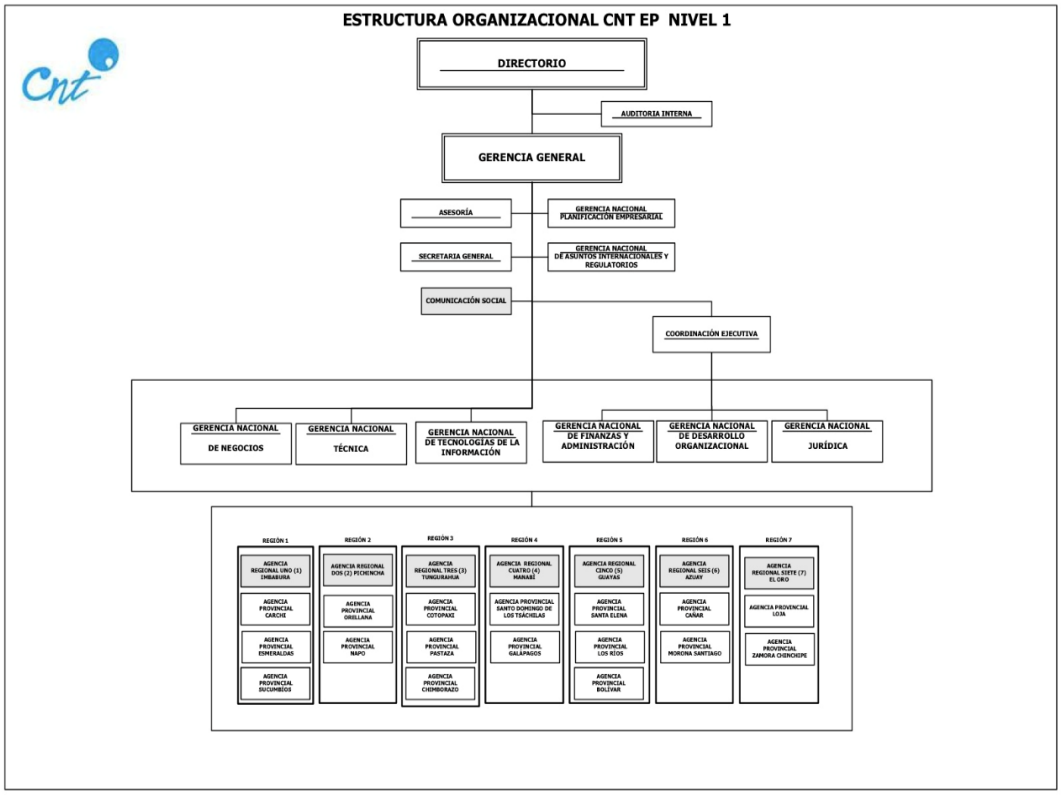
Dentro del edificio Doral existe el área del Centro de Operaciones de Redes NOC la cual vamos a utilizar como referencia ya que es un área estrictamente técnica y crítica por la información que se maneja internamente y a su vez sigue los mismos lineamientos que en forma general se utilizan en las otras áreas del edificio en temas de seguridad de la información.

En este capítulo se analizará la principal función que cumple el Centro de Operaciones de Redes NOC en el edificio Doral y en la empresa CNT EP en general, se describirá su infraestructura tecnológica, se describirá tanto su topología física como lógica, se analizará la seguridad de la información utilizada actualmente en el área buscando posibles vulnerabilidades.

2.1 Sistema de Gestión de Seguridad de la Información Utilizado Actualmente en el Edificio Doral

2.1.1 Estructura Organizacional CNT EP

A continuación se presenta en la Figura 4 la estructura organizacional de la CNT EP para llevar a cabo sus actividades y cumplir con sus objetivos estratégicos:



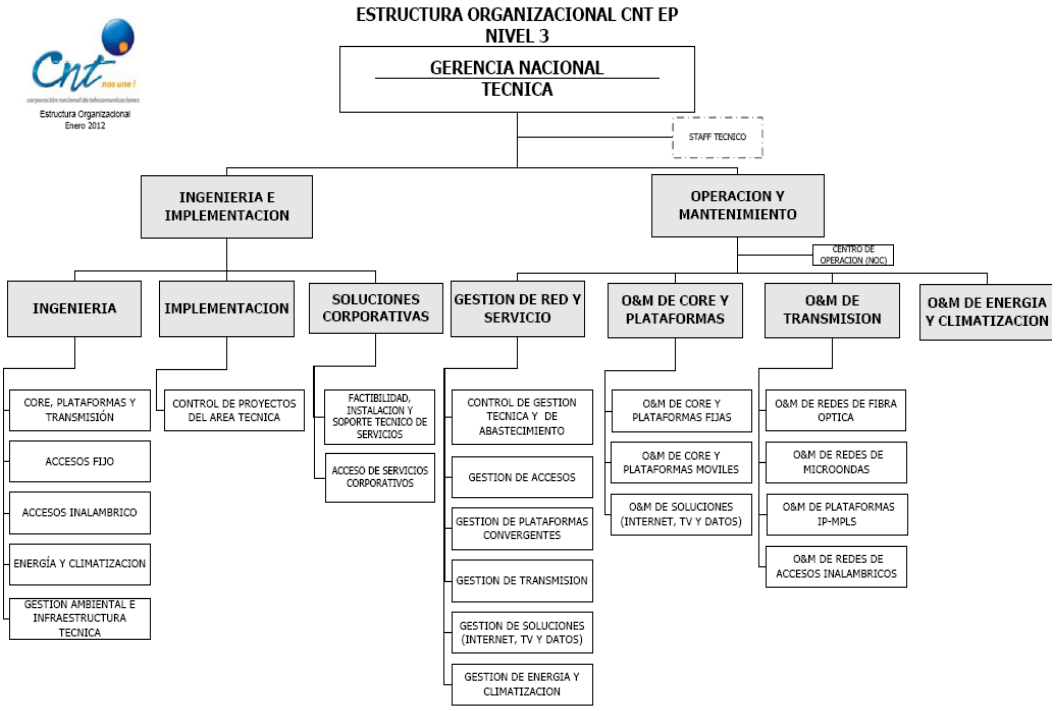


Figura 4. Estructura Organizacional CNT EP

Tomado de Universidad de los Andes, s.f.

2.1.2 SGSI Utilizado

La gerencia nacional de tecnologías de la información se encarga actualmente de la gestión del SGSI utilizado en la empresa. La CNT EP ha establecido, documentado, implementado y mantiene un Sistema de Gestión de la Seguridad de la Información, el mismo que es revisado y mejorado continuamente conforme con los requisitos de la Norma ISO 27001:2013.

2.1.2.1 Partes interesadas al SGSI

Los procesos definidos en el alcance del SGSI han identificado las siguientes partes interesadas de acuerdo a los requisitos en seguridad de la información que existen para la información que es gestionada a través de los servicios que prestan (Figura 5).

PARTES INTERESADAS	DESCRIPCIÓN
CLIENTES	Clientes corporativos (gobierno, vip, ISP's carriers y pymes) y gubernamentales.
CIUDADANÍA – SOCIEDAD	Sociedad en general, se encuentra una afectación cuando se tienen nuevos proyectos en CNT que tienen que ver con aspectos geográficos
COLABORADORES	Empleados de CNT.
ENTES DE REGULACIÓN Y CONTROL INTERNOS	Gerencia de Calidad y Procesos. Asuntos Regulatorios Gerencia Nacional Jurídica (Procesos de Contratación)
ENTES DE REGULACIÓN Y CONTROL EXTERNOS	Contraloría General del Estado. Arcotel (Permisos de frecuencias y homologaciones de equipamiento, cantidad de servicios) SNAP (Coordinación de políticas públicas sobre contratación de tecnología y telecomunicaciones) MINTEL (Ente coordinador, CNT pertenece al MINTEL como sector estratégico) Asamblea (Emisión de leyes) SENAIN (Secretaria Nacional de Inteligencia) Fiscalía General de la Nación
PROVEEDORES	Infraestructura, SW, HW y Servicios (Consultorías y horas técnicas)
OTROS	Gerencia Nacional Financiera (Costos - Presupuestos) Gerencia Nacional Técnica (Implementación de Soluciones) Gerencia General (Custodio de los contratos originales físicos) Gerencia Nacional de TI (Sistemas Transaccionales) Gerencia Nacional de Negocios (Desarrollo de productos, compra de terminales, planificación operativa) Gerencia Desarrollo Organizacional (Elaboración de procesos, Contratación/Acuerdos de Confidencialidad) Gerencia de Planificación Estratégica Activación de Servicios Desempeño de Red

Figura 5. Partes Interesadas al SGSI

Tomado de Universidad de los Andes, s.f.

2.1.2.2 Política del SGSI

La CNT EP, enmarcando sus actividades bajo los requerimientos que como empresa pública debe cumplir, trabaja para brindar servicios de telecomunicaciones manteniendo un nivel alto de protección de la información que maneja a través de su Sistema de Gestión de la Seguridad de la Información, protegiéndola mediante la pertinente gestión de riesgos, promoviendo una cultura de seguridad de la información, el cumplimiento de la normatividad vigente, requisitos legales, generando una oportuna gestión a los incidentes y aplicando mejores prácticas aplicadas a través de controles de seguridad, y garantizar la confidencialidad, integridad y disponibilidad de la información y los activos que la resguardan. La Corporación garantiza el cumplimiento, mantenimiento y mejora continua de dicho Sistema dotando de los medios y recursos necesarios e instando a todo el personal para que asuma este compromiso. La documentación del Sistema de Gestión de la Seguridad de la Información incluye los elementos que se detallan en la siguiente Pirámide de la documentación detallada en la Figura 6:

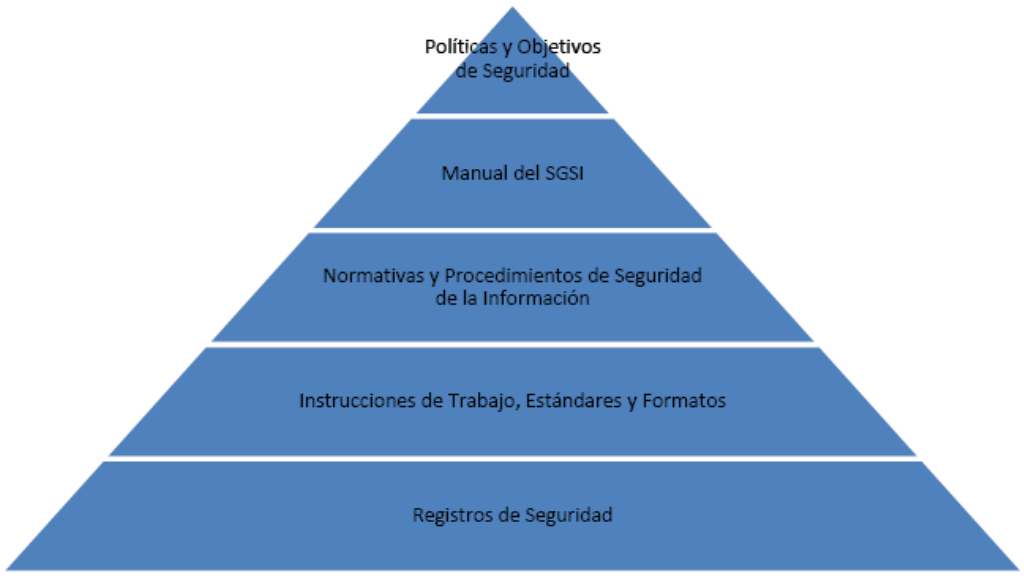


Figura 6. Documentación del SGSI de la CNT EP

Tomado de Universidad de los Andes, s.f.

2.1.2.3 Mejora del SGSI

La CNT EP, ha establecido su SGSI como un modelo que le permita mejorar continuamente incluyendo una política del SGSI, amparada por la Política de Seguridad de la Información y demás controles tanto técnicos como no técnicos así como los resultados de las auditorias y demás revisiones que continuamente arrojan no conformidades u oportunidades de mejora, las mismas que se ven traducidas en acciones preventivas y correctivas.

2.1.2.3.1 Acción Correctiva

La CNT EP, ha definido un proceso para la realización de acciones correctivas que busca eliminar las causas de las no conformidades para prevenir la recurrencia.

2.1.2.3.2 Acción Preventiva

La CNT EP, se preocupa por identificar no conformidades potenciales y sus causas por medio de revisiones periódicas realizadas por parte del Oficial de Seguridad de la Información y su equipo de trabajo (Analistas de Seguridad de la Información). Dichas revisiones se ejecutan según lo indicado en cada procedimiento que forma parte del SGSI.

2.1.3 Certificación ISO 27001

La CNT es la única empresa pública en el Ecuador con Certificación ISO 27001, que la legitima como una empresa que dispone de un sistema de seguridad de la información conforme a la Norma UNE-ISO/IEC 27001:2007. (Anexo 2). Dentro del último informe mundial de la Organización Internacional de Normalización (ISO), se han entregado 22.293 certificados ISO 27001, en el mundo, de los cuales 272 corresponden a centro y sudamérica y 5 han sido otorgados en Ecuador.

2.2 Centro de Operaciones NOC Edificio Doral

A continuación se detallarán las principales características del Centro de Operaciones de Redes NOC siendo el área que se tomará como referencia para el diseño que se realizará del sistema de gestión de la seguridad de la información.

2.2.1 Descripción Actual

El departamento de sistemas de la empresa CNT es el encargado de la administración y gestión de la red actualmente utilizada en el NOC, el área de sistemas es conformada por parte de personal de la empresa de CNT y está ubicada en el edifico Iñaquito.

El área del NOC está conformada por una red privada y en todo el edificio Doral existen 3 redes inalámbricas para disposición de los clientes. La red privada es utilizada por el área del NOC para gestionar el trabajo diario del personal que conforma el área y las redes inalámbricas son de uso público y de acceso sin restricciones.

En el área del NOC se maneja información relevante de clientes corporativos y gubernamentales como es el direccionamiento ip y la configuración de equipos de última milla que los clientes disponen en sus respectivas empresas.

En las diferentes áreas dentro del edificio Doral actualmente se dispone de personal con el suficiente conocimiento en administración de redes ya que para ingresar a dichas áreas se debe de cumplir un perfil técnico básico, esto representa una ventaja al diseñar el SGSI ya que el personal es más capacitado y por ende se obtendrá un mejor resultado en las gestión del SGSI.

2.2.2 Principales Procesos en el NOC

Existen cuatro procesos principales que se gestionan en el área del NOC los cuáles se gestionan por parte del personal que laboran en el área.

2.2.2.1 Monitoreo de Enlaces Gubernamentales y Corporativos

- Todos los clientes gubernamentales y corporativos utilizan un número de servicio conocido como piloto el cual describe el tipo de plan que tiene contratado y la información básica como nombre de la entidad, dirección ip asignada y tecnología utilizada en el enlace, toda la información de cada cliente en el sistema se la puede acceder en el aplicativo OPEN FLEXIS.

- A nivel de mpls todos los clientes tienen configurada una interfaz vlan para enrutar el enlace sea que utilice fibra o adsl en su última milla, la información configurada en la red mpls se la puede acceder por medio del aplicativo ZOC.

- Existe una herramienta informática de monitoreo llamada CACTI en la cual todas las interfaces utilizadas por todos los clientes y los nodos capa 3 a los que se pegan están ingresados en la base de datos, en este aplicativo se levantan los monitoreos y se pueden observar las gráficas de tráfico generado por el cliente en horas, días y semanas anteriores de la fecha en que se levanta el monitoreo.

- En el monitoreo se pueden observar si se han presentado caídas e intermitencias en el servicio esto dependiendo el ancho de banda contratado por el cliente.

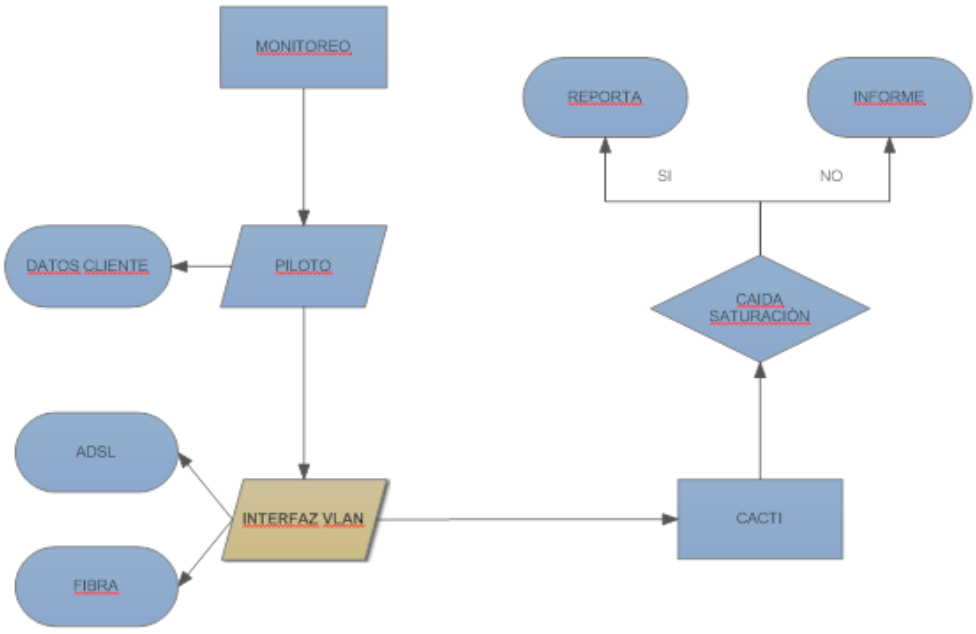


Figura 7. Diagrama de Flujo de Proceso de Monitoreo de Red

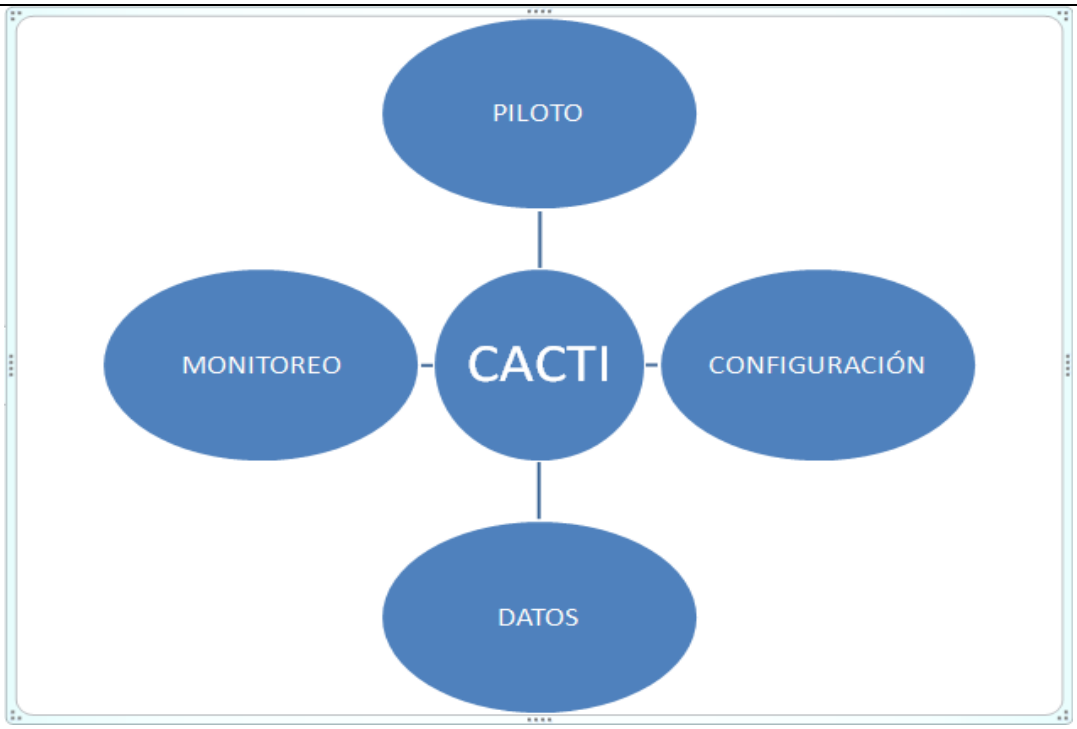


Figura 8. Monitoreo de Red

2.2.2.2 Revisión Lógica de los Enlaces

- A nivel mpls se puede verificar toda la ruta del cliente hasta nuestro equipo de última milla.

- Se puede acceder al equipo CPE (Equipo Local del Cliente) remotamente sea este un equipo router cisco para enlaces por fibra o un modem para enlaces adsl.

- Se puede cambiar las configuraciones de enrutamiento en mpls y en los equipos de última milla dependiendo de los requerimientos del cliente.

- Todo proceso realizado en la red mpls se lo realiza por medio del aplicativo ZOC.

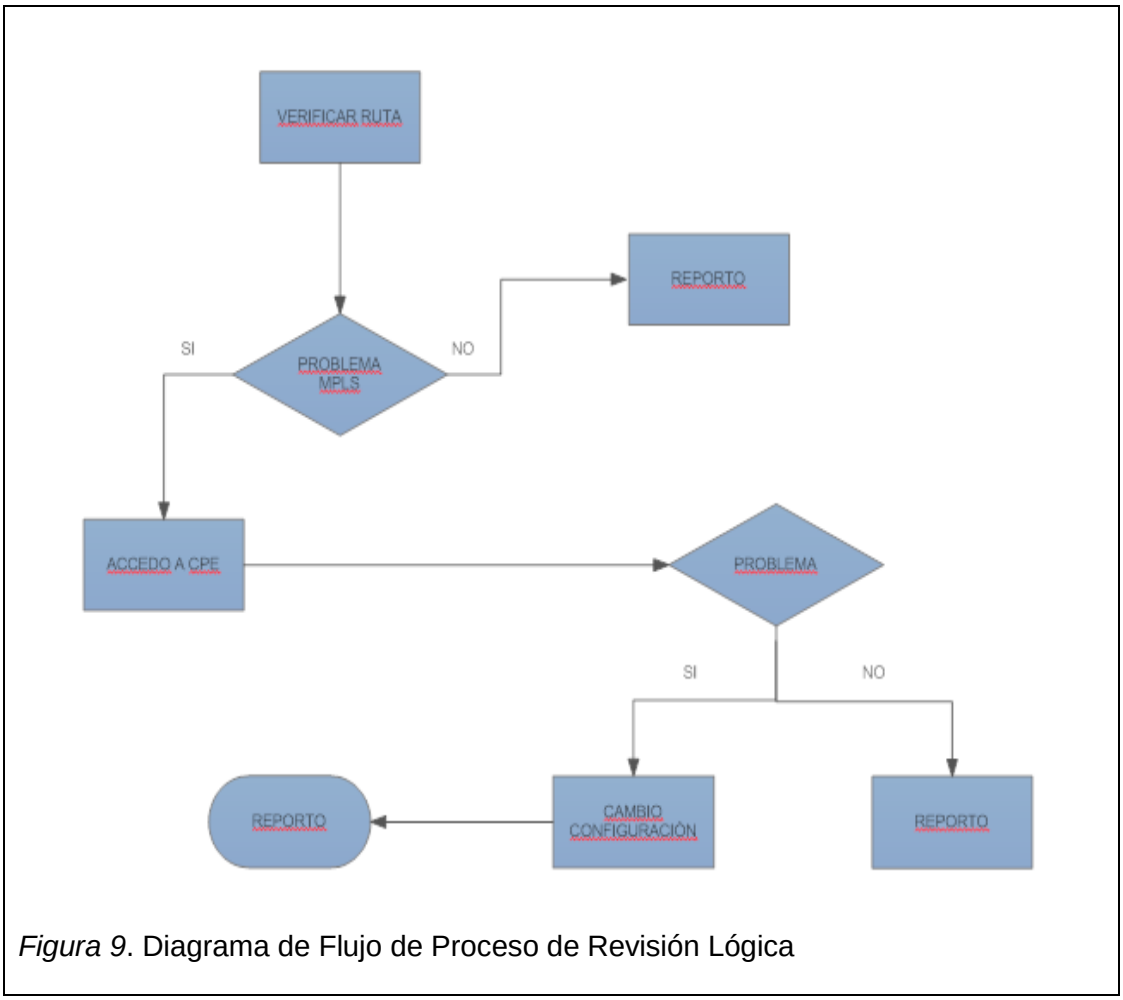


Figura 9. Diagrama de Flujo de Proceso de Revisión Lógica

Figura 10. Revisión Lógica

2.2.2.3 Revisión Física de los Enlaces

- Cuando se tiene problemas con el enlace en casos puntuales como cortes de fibra, desconfiguración de CPE`s, se escala a personal técnico de provincia al área de última milla.

- Se envía un correo informativo y se ingresa una orden de reparación en el aplicativo OPEN FLEXIS para generar órdenes.

- Personal técnico confirma reparación realizada y se revisa conjuntamente en línea operatividad del servicio y acción correctiva del problema y se cierra la incidencia generada.

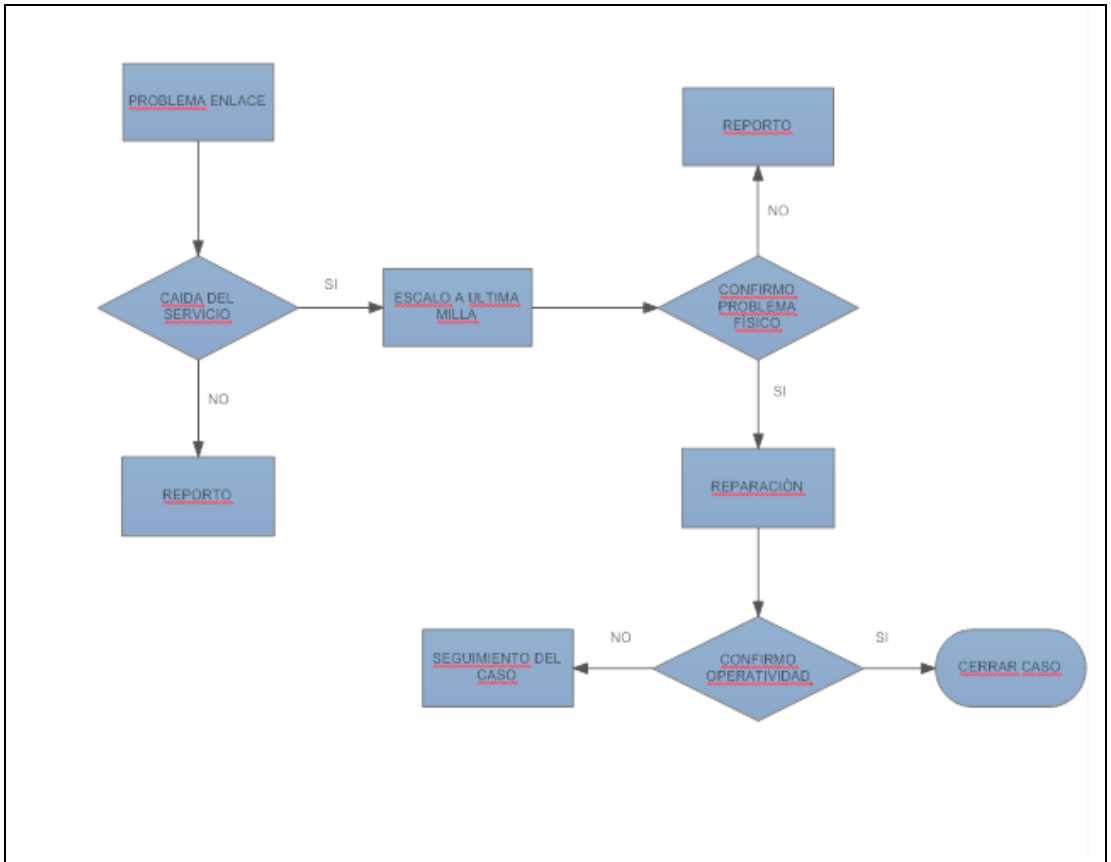


Figura 11. Diagrama de Flujo de Proceso de Revisión Física

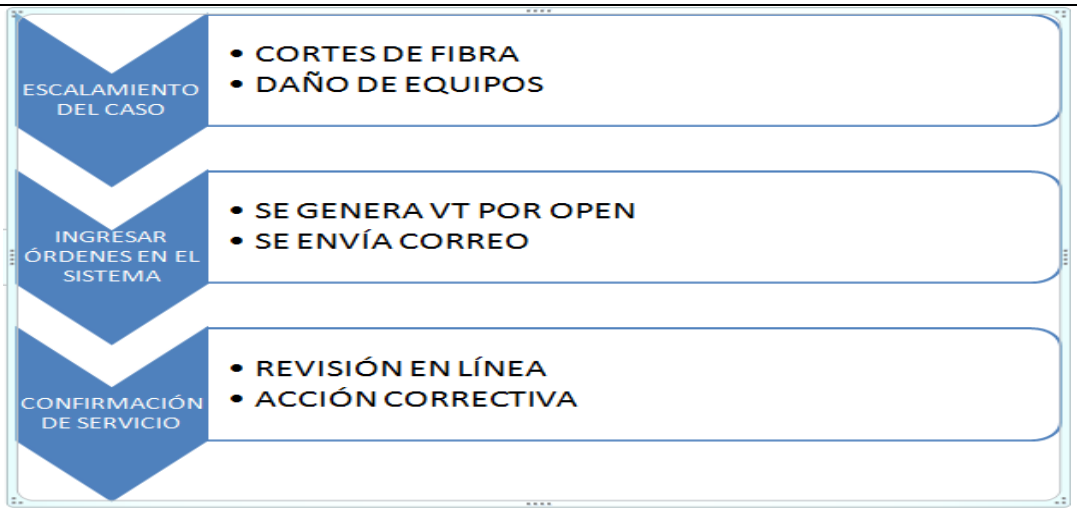


Figura 12. Revisión Física

2.2.2.4 Reparación y Mantenimiento de la Última Milla

- Cuando existe eventos masivos por ejemplo la caída de un nodo CAPA 3 al cual se peguen varios clientes, personal técnico se dirige al sitio a evaluar el problema y dar pronta solución al mismo.

- Existen eventos de mantenimiento preventivo en los cuales se alerta al cliente para poder proceder con la revisión del caso.

- Existe órdenes de trabajo facturadas en las cuales el cliente solicita revisión del enlace sin que éste presente problemas generalmente estos casos son problemas en la red interna del cliente.

- Todos los procesos de reparación y mantenimiento los realiza personal técnico del área de última milla de la provincia correspondiente donde se encuentre el enlace.

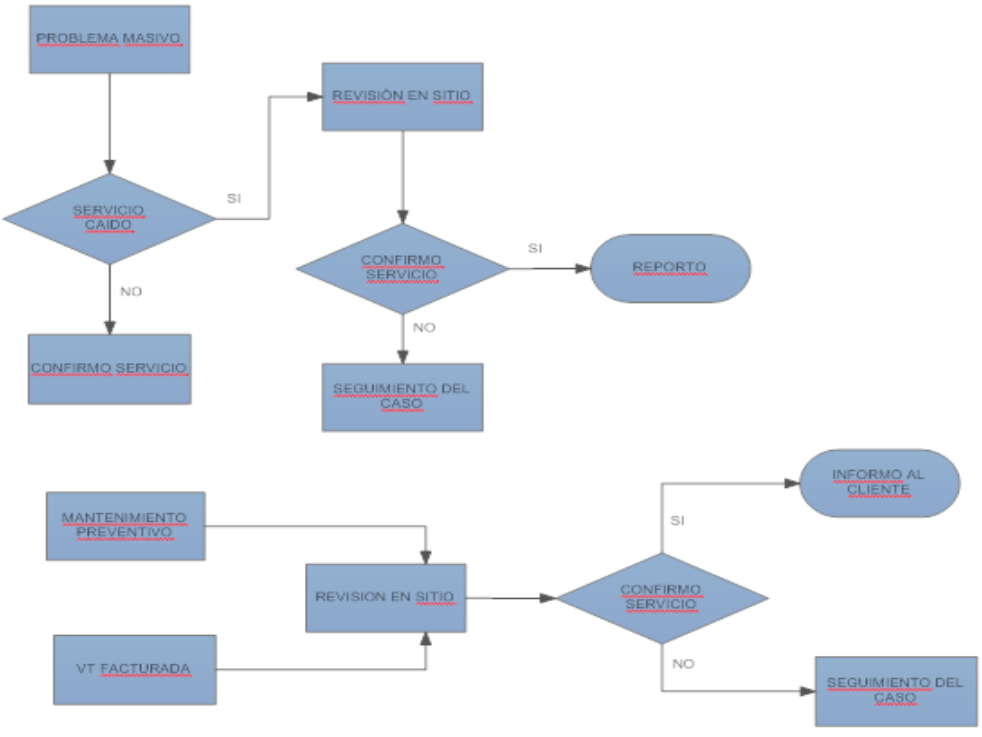


Figura 13. Diagrama de Flujo de Proceso de Reparación y Mantenimiento

Figura 14. Reparación y Mantenimiento

2.2.3 Infraestructura Tecnológica del NOC

Los servicios que brinda el área del NOC a clientes gubernamentales y corporativos a nivel nacional son enlaces de datos e internet gestionados remotamente a través de nuestra red mpls.

El principal medio de transmisión de la infraestructura de red en el edificio Doral es fibra óptica y la red se distribuye a las diferentes áreas dentro del edificio por medio de cable UTP categoría 6a.

En el área del NOC el servicio de internet es suministrado por medio de cable de fibra óptica el cual brinda mayor ancho de banda y velocidad a los usuarios que utilizan dicho servicio. El cable de fibra óptica llega a un conversor de fibra el cual convierte las señales luminosas en señales eléctricas para poder transmitir la información que se encuentra codificada por medio de cable de UTP categoría 6a, una vez convertida y decodificada la información se conecta el cable UTP entre el conversor de fibra y el router Cisco el cual es administrado por el departamento de sistemas de la empresa, en este equipo

cisco se realizan las configuraciones necesarias de enrutamiento y asignación de direcciones ip´s que la red del área utiliza para sus diferentes funciones, luego se conecta por medio de cable UTP el router cisco con el switch Dlink el cual va a expandir el servicio para todas las máquinas dependiendo del número de usuarios y el número de puertos disponibles en el switch, estas máquinas a su vez se conectan por medio de cable UTP al switch y las mismas se configuran y utilizan según el rol desempeñado por el usuario.

Las redes inalámbricas que son utilizadas por los usuarios de las diferentes áreas del edificio y las personas que ingresan a la infraestructura que disponen de un equipo con conexión wi-fi son distribuidas desde diferentes equipos módems ubicados estratégicamente en el edificio para abarcar todo el espacio físico disponible, estos equipos son administrados de igual forma por el departamento de sistemas de la empresa y tienen la misma topología física de los equipos utilizados dentro del área del NOC a diferencia que la conexión con los equipos que soportan conexión wi-fi se da inalámbricamente y no por cable UTP y no tiene restricción para validar la conexión ya que estas redes son de uso público.

2.2.3.1 Topología Física

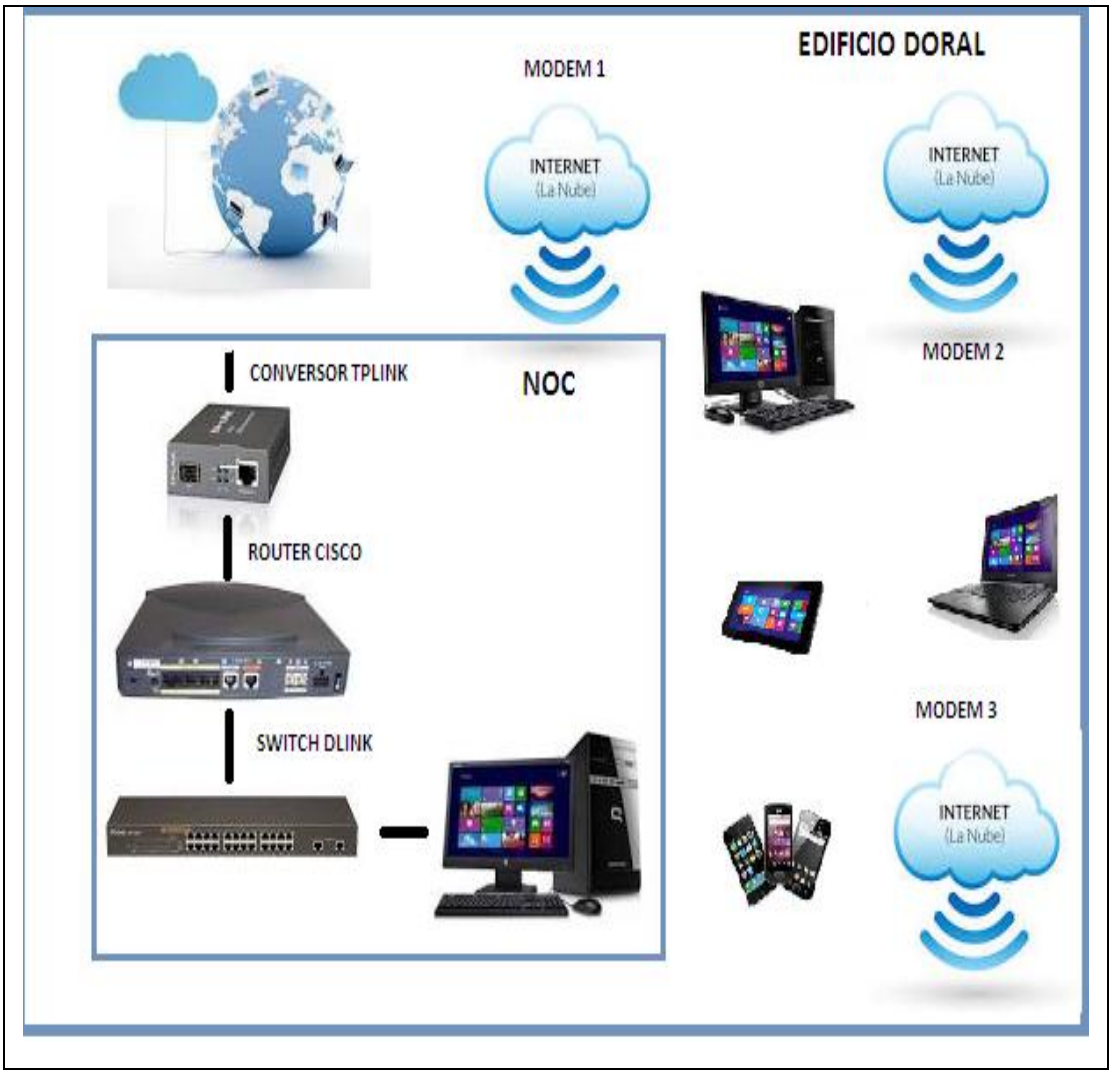
La infraestructura de red utilizada en el NOC se describe a continuación:

- El conversor de fibra
- El router cisco
- El switch Dlink
- El computador

Son los equipos principales utilizados en el área dentro del espacio físico asignado para el NOC en el edificio Doral, las redes inalámbricas están distribuidas en zonas determinadas del edificio Doral para que las redes wi-fi puedan ser accedidas por los usuarios en todo el edificio y por los clientes en general que visitan el edificio (Figura 15).

- Cable de fibra óptica
- Cable UTP
- Red Inalámbrica (Wi-Fi)

Son los medios de transmisión utilizados en el área del NOC, la fibra óptica es utilizada para acceder a la red del edificio Doral en general, el cable UTP es utilizado para expandir la red dentro del edificio a todas las áreas que funcionan en el edificio, la red inalámbrica para brindar servicio de internet sin restricción al público y a los usuarios de las diferentes áreas que se encuentran dentro del edificio.



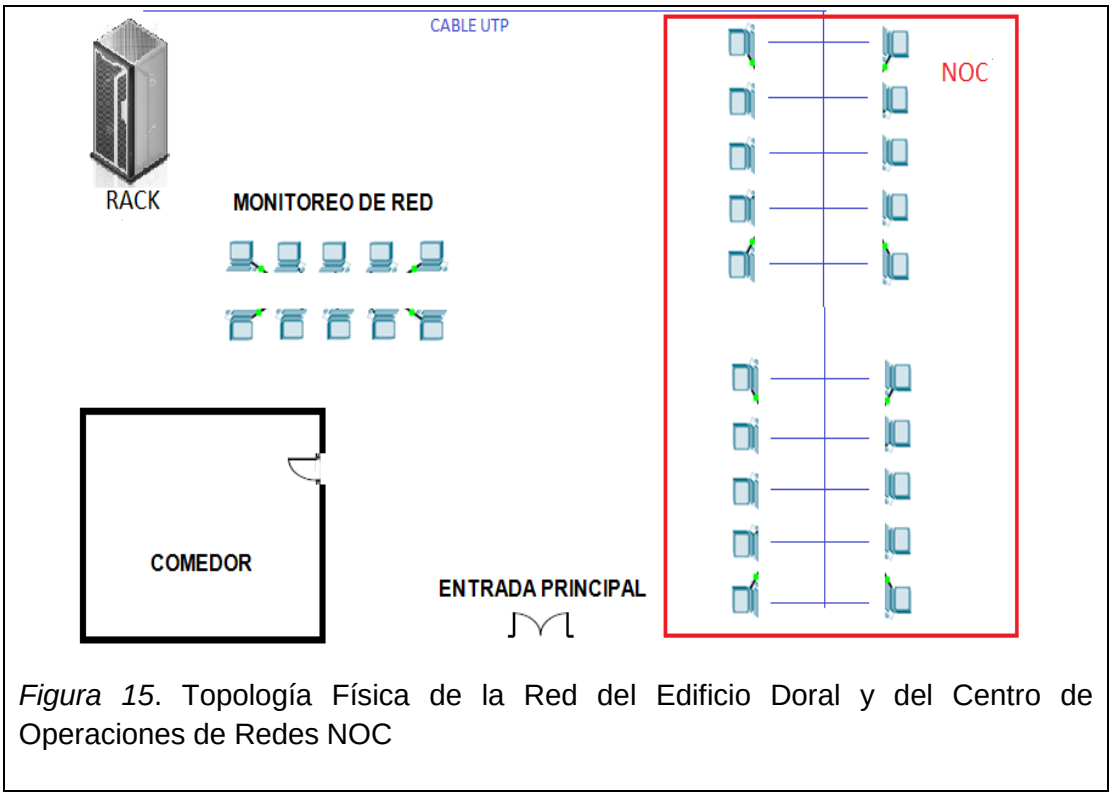


Figura 15. Topología Física de la Red del Edificio Doral y del Centro de Operaciones de Redes NOC

2.2.3.2 Topología Lógica

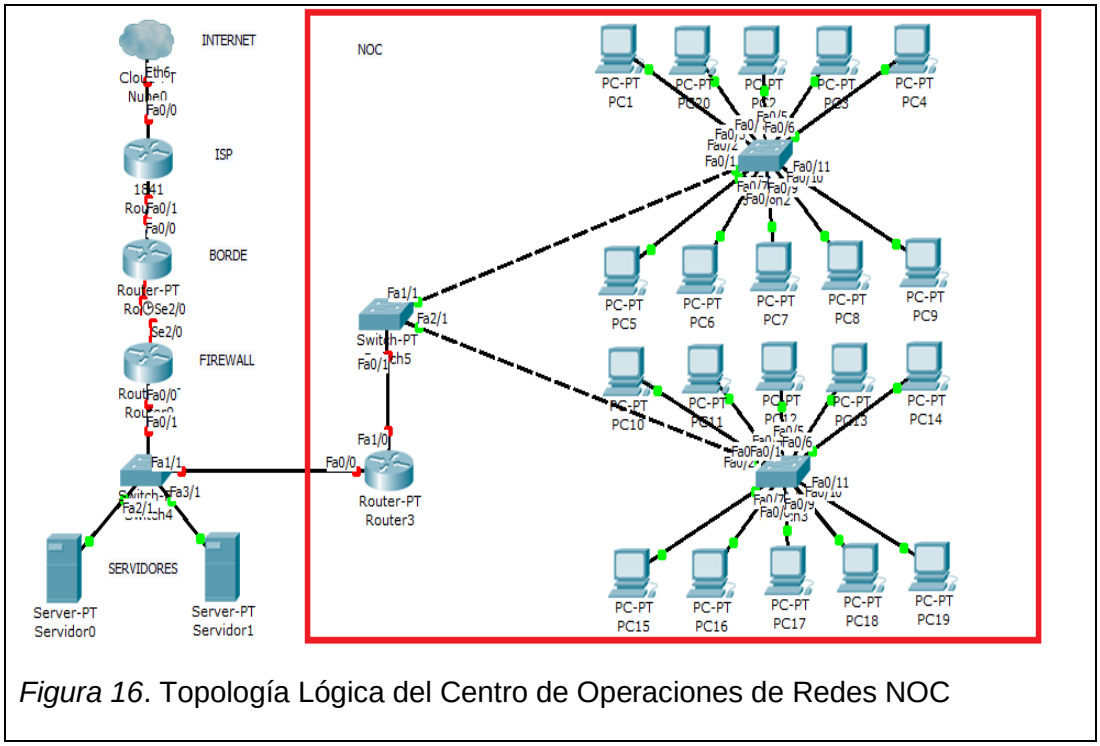


Figura 16. Topología Lógica del Centro de Operaciones de Redes NOC

Como se observa en la topología lógica en la Figura 16 la red del Área del NOC está conformada por un router, tres switchs y 20 computadores, el router considerado de borde para nuestra área se conecta a un switch considerado de distribución el cuál expande la red conectándose a los otros dos switchs que serían considerados los de acceso, los mismos que distribuyen las conexiones a 10 computadores cada uno.

Los equipos de la red principal del piso en nuestro caso los equipos visibles fuera del margen del área del NOC en la figura 14, se ubican fuera del área física del NOC y distribuyen el cableado a las otras áreas dentro del piso por conductos y cableado transportado por el techo falso.

2.2.3.3 Direccionamiento IP

Por motivos de políticas de seguridad internas de la Corporación Nacional de Telecomunicaciones y por la información crítica que la misma maneja en sus diferentes áreas dentro del edificio Doral no se pueden detallar los datos reales del direccionamiento ip que se utiliza, en el caso de ser necesario para los fines pertinentes dentro del proyecto se utilizará un rango de direcciones ip´s para fines demostrativos (Tabla 1).

Tabla 1. Direccionamiento IP NOC

DIRECCIONAMIENTO IP	
DESCRIPCIÓN	**SUBRED**
RED LOCAL	10.10.5.0/24
WIRELESS INVITADOS	10.10.6.0/24
WIRELESS MÓVILES	10.10.7.0/24
WIRELESS USUARIOS	10.10.8.0/24
RED DE INTERNET	192.168.10.30/29

2.2.3.4 Equipos de Red

A continuación en la Tabla 2 se describen los equipos que conforman la red actualmente utilizada en el NOC:

Tabla 2. Equipos de Red NOC

DESCRIPCIÓN	CANTIDAD	ESTADO
CONVERSOR TP-Link WDM 10/100Mbps	1	ACTIVO
ROUTER CISCO 800	1	ACTIVO
SWITCH D-Link 16 PUERTOS	3	ACTIVO
COMPUTADOR INTEL CORE	20	ACTIVO

2.2.3.4.1 Conversor TP-Link WDM

Figura 17. Conversor TP-Link WDM

Tomado de Universidad de los Andes, s.f.

1. Auto negociación de 10/100Mbps y auto MID / MID-X para el puerto TX.
2. Proporciona la configuración del switch de Modo de transferencia Medio Dúplex/Dúplex Completo para el puerto FX.

3. El paso de enlace de fallas y errores minimizan oportunamente la pérdida causada por la falla en el enlace.
4. Adopta la tecnología WDM, transmite y recibe datos en una sola fibra.
5. Extiende la distancia de fibra hasta 20-60km.
6. Fácil de ver los indicadores LED que proporcionan el estado para supervisar fácilmente la actividad de la red.
7. Fuente de alimentación externa.
8. Compatible con los estándares 802.3u 10/100 Base-TX, 100Base-FX.
9. WDM TX 1310nm.
10. WDM RX 1550nm.
11. Máximo consumo de potencia 2,41W.

2.2.3.4.2 Router Cisco 800

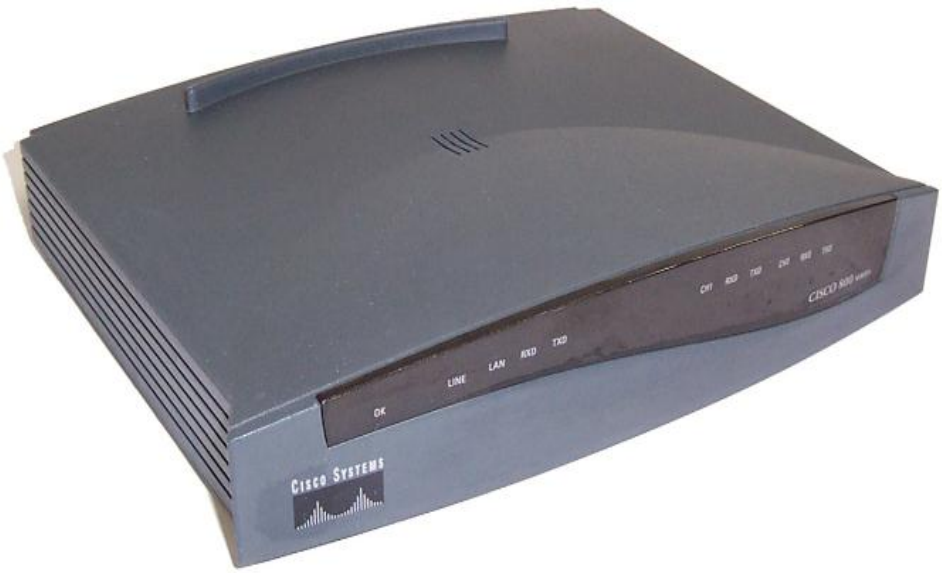


Figura 18. Router Cisco 800

Tomado de Universidad de los Andes, s.f.

1. Los routers de la serie Cisco 800 amplían la potencia de la tecnología Cisco IOS a las oficinas pequeñas.
2. Los routers ISDN (RDSI) de la serie Cisco 800 permiten a los clientes sacar el mayor partido a los servicios de valor añadido, como servicios de red gestionados, redes virtuales privadas (VPN), aplicaciones de punto de venta (POS) y acceso seguro a Internet.
3. Se basa en Ethernet y Fast Ethernet.
4. La administración de corriente del cisco maneja los siguientes voltajes AC120/230 V (50/60 Hz).
5. Información de Protocolo de Routing (RIPv1 y RIPv2).
6. Network Address Translation (NAT) y Port Address Translation (PAT).
7. Dynamic Host Control Protocol (DHCP) servidor/relay/cliente.
8. Listas de control de Acceso (ACLs).
9. 802.11b/g.
10. Alcance interior: 1 Mbps 100 metros.
11. Wi-Fi Protected Access (WPA).
12. DRAM máxima 64MB.
13. Memoria Flash máxima 20MB.
14. Voltaje de entrada AC: 100 a240 VAC.
15. Frecuencia: 50 a60 Hz.
16. Potencia máxima de salida: 26W.
17. Voltaje de salida: 5 y 12V.
18. Temperatura operacional: 0 a 40°C.

2.2.3.4.3 Switch D-Link 16 Puertos

Figura 19. Switch D-Link 16 Puertos

Tomado de Universidad de los Andes, s.f.

1. Potentes pero fáciles de utilizar, estos conmutadores permiten la conexión Gigabit de hasta 16 ordenadores o dispositivos de red.
2. Ahorro de energía de hasta 73%* con tecnologías D-Link Green.
3. Dispositivos de elevado rendimiento.
4. Ahorro de espacio y dinero.
5. Control de flujo.
6. IEEE 802.3x control de flujo proporciona una transferencia de datos fiables.
7. Capacidad de conmutación 3.2Gbps.
8. Auto-negociación puertos que faciliten la integración inteligente entre 10 Mbps, 100 Mbps de hardware.
9. Memoria RAM 512Kbps.
10. Potencia de consumo 13,4W.

2.2.3.4.4 Computador Intel Core.

Figura 20. Computador Intel Core

Tomado de Universidad de los Andes, s.f.

1. Procesador Intel Core i7 de 3,6 GHz 4ta generación.
2. Memoria 4 Gb.
3. Disco duro 1000 Gb.
4. DVD writer.
5. Lector de memorias.
6. Memoria RAM 2Gb.
7. Teclado multimedia.

2.2.3.5 Herramientas Utilizadas para la Gestión en el Área del NOC (Software)

El área de sistemas SIS de la CNT administra todos los gestores que se utilizan en las diferentes áreas que conforman la empresa, el área de SIS se encuentra en el edificio Iñaquito y administra remotamente cualquier petición que se solicite.

El software es almacenado en un servidor de aplicaciones gestionado por el área de SIS, este servidor se encuentra físicamente en el edificio Iñaquito y únicamente es administrado por el área de Sistemas por lo que cualquier petición o solicitud que involucre a los gestores utilizados en las diferentes áreas de la CNT en cualquier sede se la procesa de manera remota.

Los principales gestores que se utilizan en el área del NOC son:

2.2.3.5.1 ZOC

Es un popular emulador de terminal de computadora y software de cliente telnet desarrollado para sistemas operativos Microsoft Windows and Apple Macintosh OS X (Mac OS X), que es compatible con telnet, módem, SSH 1 y 2, RDSI , serial , TAPI , Rlogin y otros medios de comunicación.

Con este software se puede acceder a la red mpls de la CNT, conectándonos con los nodos capa 3, switchs capa 2 y equipos CPE en toda la red administrada por la CNT a nivel nacional. Para poder acceder a la red mpls cada analista en el área tiene su usuario y clave mpls, dependiendo del cargo y

función desempeñado se otorgan privilegios para poder realizar configuraciones dentro de los equipos.

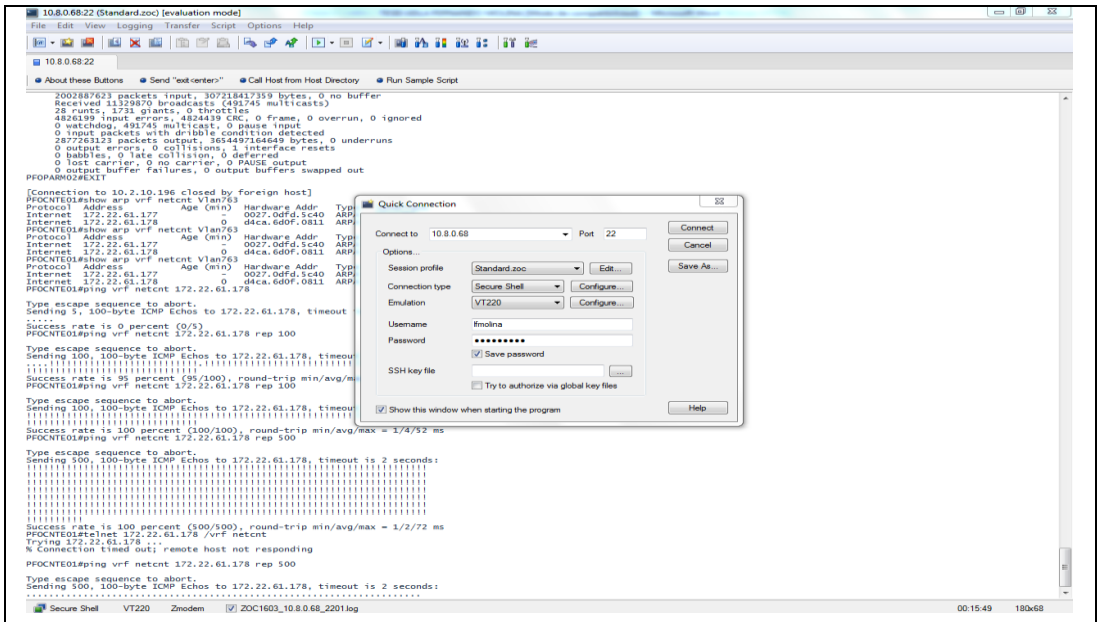


Figura 21. Interfaz ZOC

2.2.3.5.2 OPEN FLEXIS

Es una herramienta utilizada para la prestación del servicio de telefonía fija que se utiliza para controlar el inventario de los elementos que conforman la red de telefonía de CNT, normalizar los procesos de gestión de cartera y recaudos, controlar y clasificar los servicios de larga distancia y facilitar las decisiones relacionadas con el proceso de compensación con otros operadores.

En nuestro caso se utiliza como una herramienta de búsqueda de información de cada cliente a nivel nacional, cada cliente tiene un número de servicio conocido como piloto el cuál al ser ingresado en el gestor nos detalla información como dirección de la entidad, tipo de servicio contratado, características físicas del enlace, órdenes de trabajo ingresadas, etc.

Para poder acceder al gestor cada analista en el área tiene su usuario y clave open la cuál es administrada por el departamento de sistemas de la entidad.

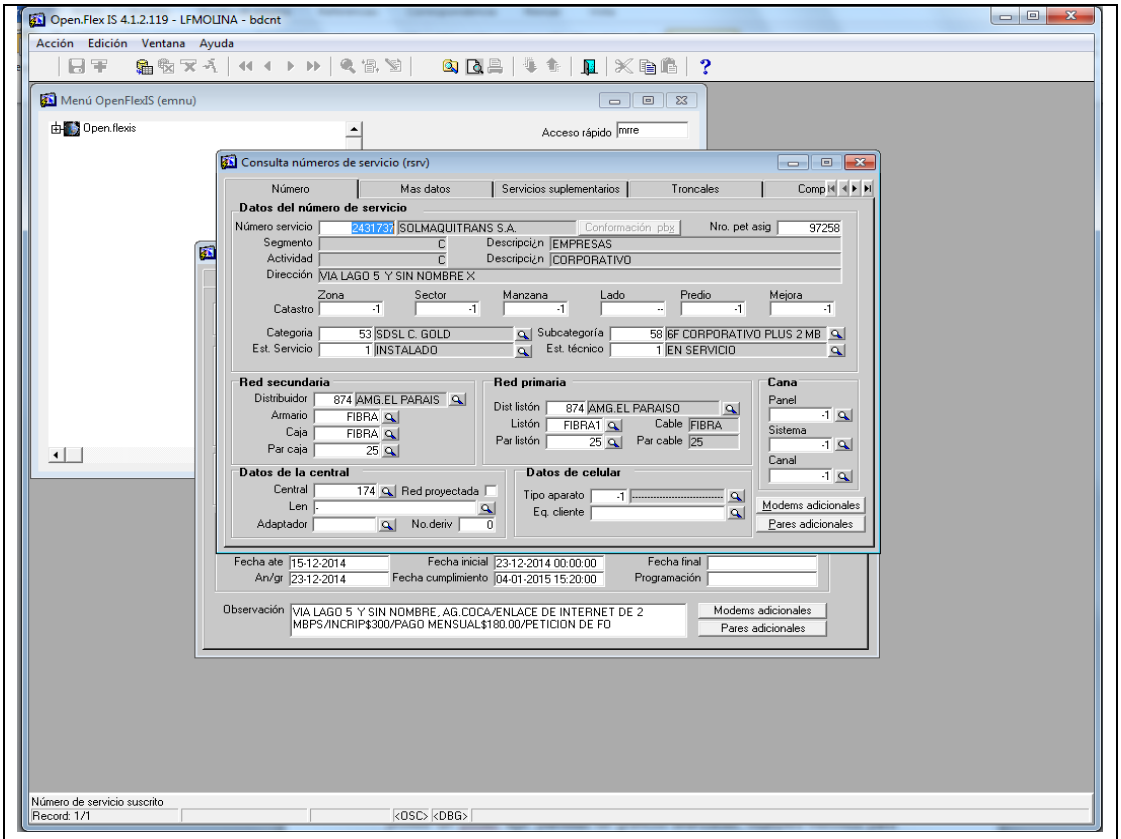


Figura 22. Interfaz OPEN FLEXIS

2.2.3.5.3 CACTI

Es una completa solución para la generación de gráficos en red, diseñada para aprovechar el poder de almacenamiento y la funcionalidad para gráficas que poseen las aplicaciones RRDtool. Esta herramienta, desarrollada en PHP, provee un pooler ágil, plantillas de gráficos avanzadas, múltiples métodos para la recopilación de datos, y manejo de usuarios. Tiene una interfaz de usuario fácil de usar, que resulta conveniente para instalaciones del tamaño de una LAN, así como también para redes complejas con cientos de dispositivos.

Esta herramienta se utiliza para levantar monitoreos de los enlaces a nivel nacional, los resultados son utilizados para verificar si existen caídas o saturación en los servicios.

Para acceder a este gestor se utiliza un usuario y clave común, existe la alternativa que los clientes a nivel nacional de requerir pueden contratar este

monitoreo para administrarlo por si mismo esto aprobando un contrato y acuerdo con el área comercial de la CNT.

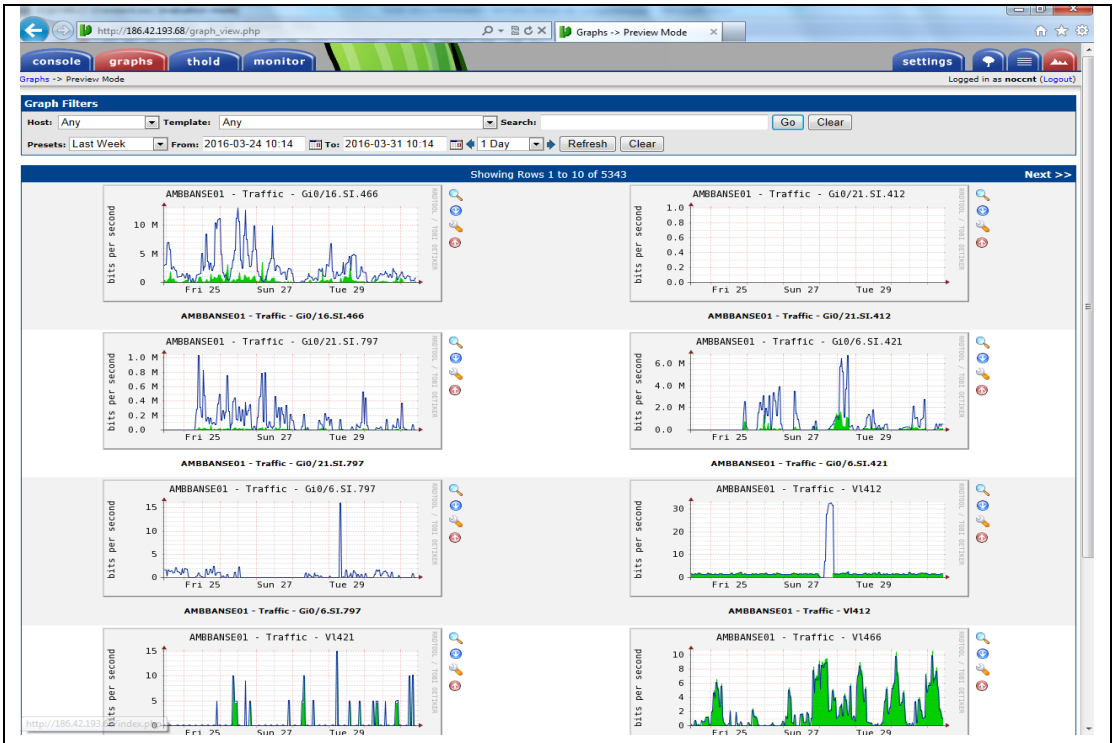


Figura 23. Interfaz CACTI

Tabla 3. Procesos y Aplicativos

PROCESO	APLICATIVO
MONITOREO DE ENLACES GUBERNAMENTALES Y CORPORATIVOS	
Generar gráficas de los enlaces	CACTI
Verificar caídas del servicio en el monitoreo	CACTI
Verificar saturación del servicio en el monitoreo	CACTI
REVISION LÓGICA DE LOS ENLACES	
Verificación de datos del cliente	OPEN FLEXIS
Acceder a la red mpls	ZOC
Verificar enrutamiento	ZOC
Cambiar configuración de equipos	ZOC
REVISION FÍSICA DE LOS ENLACES	
Generar órdenes de visita técnica	OPEN FLEXIS
Verificar estado de la reparación	OPEN FLEXIS
Realizar pruebas del servicio	ZOC

REPARACIÓN Y MANTENIMIENTO DE LA ÚLTIMA MILLA	
Generar órdenes de visita técnica	OPEN FLEXIS
Verificar estado del mantenimiento	OPEN FLEXIS
Realizar pruebas del servicio antes y después del mantenimiento	ZOC

2.2.4 Estado Actual de la Seguridad de la Información en el NOC

A continuación se detallarán los problemas comunes encontrados en el área del NOC:

2.2.4.1 Problemas Actuales en el Área del NOC

2.2.4.1.1 Problemas en el Proceso de Monitoreo de los Enlaces del área del NOC:

- Para buscar los datos de cada cliente en el sistema se utiliza el gestor OPEN FLEXIS, cuando existen problemas con el gestor no se tiene acceso a esta información.

- Existen ocasiones cuando el usuario del gestor OPEN FLEXIS de cada usuario del NOC se bloquea y no se puede acceder a ésta herramienta, este bloqueo se da cuando se ingresa la clave incorrecta por varias ocasiones.

- Los datos del cliente en el gestor OPEN FLEXIS no coinciden con los configurados a nivel de mpls (interfaz vlan).

- Para buscar los enlaces en el gestor CACTI se debe de tener ingresada la información de todos los equipos Capa 3 a los cuales se pegan los clientes que se requieren levantar monitoreos, existen casos en los cuales estos equipos no están ingresados en el gestor.

- No se puede acceder al gestor CACTI cuando se pierde conexión con el mismo.

- Las gráficas creadas para monitorear los enlaces en ocasiones no grafican tráfico generado aunque el enlace este up.

- Los clientes disponen de monitoreos personalizados en los cuales el accede a la información del monitoreo levantado sin necesidad de solicitar la información al NOC, en ocasiones las gráficas no muestran tráfico generado y el cliente reporta daño en su gestor de monitoreo.

2.2.4.1.2 Problemas en el Proceso de Revisión Lógica de los Enlaces del área del NOC:

- Existen problemas con la búsqueda de la información del cliente cuando la misma no coincide en el sistema OPEN FLEXIS con la configuración en mpls.

- En ocasiones la ruta mpls del cliente se encuentra mal configurada o borrada.

- Se pierde el acceso al equipo CPE por desconfiguración del mismo.

- Cuando el cliente solicita configuraciones adicionales directamente en el CPE el caso se escala al área de soporte N2.

2.2.4.1.3 Problemas en el Proceso de Revisión Física de los Enlaces del área del NOC:

- La información de la dirección física donde se encuentra instalado el enlace en ocasiones está errónea.

- Existen cortes de fibra que demoran la reparación.

- En el sistema OPEN FLEXIS no se puede ingresar las órdenes de trabajo por mal funcionamiento del gestor.

- Se debe de escalar el caso a la provincia correspondiente.

- Se reasigna el caso cuando el problema vuelve a reportarse.

- El tiempo de solución del problema cuando es escalado a personal de última milla en ocasiones es demasiado tardío.

2.2.4.1.4 Problemas en el Proceso de Reparación y Mantenimiento de la Última Milla del área del NOC:

- Los problemas masivos no son identificados pronto.

- Existen clientes identificados como AAA que en ocasiones su servicio es afectado por eventos masivos, estos clientes deben de tener prioridad para acelerar la solución del problema.

- Cuando existen eventos de mantenimiento preventivo se debe de verificar la operatividad de los enlaces pegados a los equipos que serán revisados antes y después del mantenimiento.

- Mientras no se confirmen todos los servicios operativos después del mantenimiento esta orden no puede ser resuelta.

- Se debe confirmar el daño vía telefónica con el cliente realizando pruebas de primer nivel antes de escalar el caso para la revisión en sitio.

2.2.4.1.5 Problemas en la Infraestructura Tecnológica:

- Daños en equipos de red.

- Desconfiguración de los equipos de red.

- Problemas de conexión con los gestores OPEN FLEXIS, CACTI y ZOC.

Tabla 4. Problemas en el Área del NOC

RESUMEN DE PROBLEMAS EN EL ÁREA DEL NOC (PROCESOS)		
ACTIVIDAD	**TIPO**	**PROCESO**
		Monitoreo de Enlaces Gubernamentales y Corporativos
Configuración	Tecnológico	Desconfiguración de los gestores
Acceso	Gestión	Bloqueo en el acceso a los gestores
Regularización	Gestión	Datos del cliente incorrectos
Regularización	Gestión	Información incompleta en el gestor
Monitoreo	Tecnológico	Problemas gráficos en el gestor
		Revisión Lógica de los Enlaces del área del NOC
Configuración	Gestión	Datos erróneos en mpls
Configuración	Gestión	Desconfiguración de enrutamiento
Configuración	Tecnológico	Desconfiguración de CPE
		Revisión Física de los Enlaces del área del NOC
Regularización	Gestión	Dirección del cliente errónea
Revisión	Gestión	Tiempo excesivo de revisión
Configuración	Tecnológico	Falla del gestor
Escalamiento	Gestión	Equivocación en escalamiento a provincia
Resolución	Gestión	Reasignación del caso
		Reparación y Mantenimiento de la Última Milla
Revisión	Gestión	Eventos masivos no identificados
Reparación	Gestión	Tiempo excesivo de reparación
Reparación	Tecnológico	Revisión de enlaces antes y después del mantenimiento
RESUMEN DE PROBLEMAS EN EL ÁREA DEL NOC (INFRAESTRUCTURA TECNOLÓGICA)		
ACTIVIDAD	***TIPO***	***INFRAESTRUCTURA EXTERNA***
		Medio de Transmisión
Transmisión	*Tecnológico*	Daño en medio de transmisión
Transmisión	*Gestión*	Ancho de banda insuficiente
		Equipos de Red

Gestión	*Tecnológico*	Daño en equipo de red
Gestión	*Tecnológico*	Desconfiguración en equipo de red
ACTIVIDAD	***TIPO***	***INFRAESTRUCTURA INTERNA***
		Software de Gestión
Gestión	*Gestión*	Bloqueo en el acceso a los gestores
Gestión	*Tecnológico*	Daño en los gestores

3. Capítulo III. Definición del Sistema de Gestión de Seguridad de la Información para la Matriz Doral CNT

Tomando como referencia los problemas encontrados en el área del NOC se analizará el estado actual de la seguridad de la información proponiendo posibles soluciones basándonos en los dominios y los puntos más importantes que la norma INEN-ISO/IEC 27001 considera indispensables mantener para administrar un sistema de gestión de la seguridad de la información SGSI en las empresas públicas ecuatorianas, toda la información podrá documentarse en el sistema Alfresco.

3.1 Alfresco

3.1.1 Sistema Alfresco

Es un sistema de administración de contenidos de código fuente libre, Alfresco es utilizado como software de gestión documental para documentos, páginas web, registros, imágenes y desarrollo colaborativo de contenido.

Características:

- Gestión de documentos.
- Gestión de contenido web (incluyendo aplicaciones web y virtualización de sesiones).
- Gestión de registros.
- Gestión de imágenes.
- Soporte de varios idiomas.
- Empaquetamiento de aplicación portable.

3.1.2 Funcionalidad

La norma INEN-ISO/IEC 27001 recomienda definir procesos para el manejo de la documentación que conforma el SGSI que permitan proteger, controlar y mantener en disponibilidad dicha documentación para los usuarios de la empresa.

La gestión de dicha documentación contiene las siguientes actividades:

- Prevenir el uso no intencionado de documentos obsoletos.
- Asegurar que la distribución de documentos esté controlada.
- Asegurar que la documentación esté disponible para toda persona que lo necesite.
- Asegurar que los documentos sean fácilmente identificados.
- Asegurar que los cambios en los documentos sean identificados.
- Revisar, actualizar y aprobar documentos.

3.1.3 Alfresco como Herramienta de Apoyo para el Diseño de un SGSI

La gestión de la documentación se la puede realizar de forma manual con documentos impresos, archivos digitales o herramientas electrónicas.

Alfresco ayudará en la gestión de contenidos de la organización, la automatización de procesos empresariales y la gestión de documentos críticos.

Entre las principales funciones que Alfresco ofrecerá en la gestión de la documentación en el SGSI se encuentran:

- Se visualiza archivos en línea sin necesidad de descargarlos, soporta archivos de Office, imágenes y archivos de audio y video.
- Flujo de trabajo eficaz para la gestión de procesos empresariales.
- Permite la edición de archivos en línea lo cual permite a su vez la actualización de dicho archivo y el almacenamiento de su nueva versión.
- Permite la asignación de diversas propiedades a los documentos como la asignación de títulos, descripciones, autor, fechas, etc; esto para facilitar con la creación de grupos de documentación según sus atributos o a su vez personalizar documentos.

3.2 Análisis de la Situación Actual en el Área del NOC

3.2.1 Procesos Manejados en el Área

- En todos los procesos gestionados en el área el uso de gestores (software) para desarrollar determinadas funciones es indispensable, uno de

los principales problemas es la indisposición de las herramientas causada por la desconfiguración del software y la inaccesibilidad a los gestores por problemas en la administración y uso de herramienta.

- La información disponible del cliente en los gestores que se utilizan para desarrollar determinadas funciones dentro del área en ciertas ocasiones está incompleta o equivocada, se debe confirmar la información actualizada que se registre del cliente en el sistema Open antes de realizar la revisión del servicio reportado con problemas.

- Los equipos instalados en las centrales y donde el cliente pueden sufrir de daños físicos o desconfiguraciones lógicas, al tratarse de un daño se requiere de la revisión en sitio por parte de personal técnico de última milla y al tratarse de desconfiguraciones se puede solventar el problema remotamente, son pocos los casos que se requiere visita técnica en sitio para reconfigurar equipos.

- Cuando los casos son escalados a personal técnico de última milla existe el problema que la revisión o reparación de los enlaces puede demorar demasiado tiempo incumpliendo los estándares de tiempo establecidos en los contratos con los clientes (Acuerdos de Nivel de Servicio SLA’s).

- Existen eventos masivos y mantenimientos preventivos que causan la caída de todos los servicios que se conectan al nodo o equipo involucrado, al tratarse de eventos masivos se debe de dar la prioridad y atención que amerita el caso para que los enlaces puedan ser recuperados inmediatamente, al tratarse de mantenimientos preventivos se debe verificar operatividad de todos los servicios antes y después del mantenimiento, generalmente los mantenimientos se los realiza en horas de la madrugada cuando los enlaces no son utilizados por el cliente.

3.3 Diseño del Sistema de Gestión de Seguridad de la Información (SGSI) del Centro de Operaciones de Redes NOC

Para desarrollar el diseño del SGSI propuesto en el proyecto se tomará como referencia las políticas recomendadas en el esquema gubernamental de seguridad de la información para poder diseñar e implementar un sistema de gestión de seguridad de la información en empresas públicas nacionales, dichas políticas están contempladas en la norma INEN-ISO/IEC 27001.

3.3.1 Políticas y Dominios Utilizados

A continuación en la Tabla 5 se describirán todas las políticas y dominios recomendados utilizar por el esquema gubernamental de seguridad de la información para diseñar e implementar un SGSI (Anexo 3), se analiza el motivo por el cual se utiliza o no cada dominio según los requerimientos de seguridad de la información del área del NOC.

Tabla 5. Políticas y Dominios Utilizados

DOMINIO	***SELECCIÓN***	***JUSTIFICACIÓN***
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		
Documento de la Política de la Seguridad de la Información	SI	Este dominio es importante considerar pues este documento representará todas las directrices que el SGSI gestionará para el manejo de las políticas diseñadas.
Revisión de la Política	SI	Es importante realizar revisiones periódicas de las políticas implementadas.
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		
Compromiso de la máxima autoridad de la institución con la seguridad de la información	SI	Los directivos del área del NOC conforman el comité de seguridad de la información.
Coordinación de la Gestión de la Seguridad de la Información	SI	La coordinación y gestión de las políticas propuestas está a cargo del comité de seguridad. Se debe aplicar la Norma ISO/IEC utilizada para el desarrollo de las políticas conjuntamente con el esquema gubernamental.
Asignación de responsabilidades para la seguridad de la información	SI	Se asignan funciones a los integrantes del comité de seguridad.
Proceso de autorización para	NO	La posibilidad de implementar

nuevos servicios de procesamiento de la información		nuevos servicios dentro del área es nula ya que la prestación de servicios depende del área comercial y la implementación de dichos servicios de las altas gerencias de la empresa.
Acuerdos sobre Confidencialidad	SI	Los acuerdos de confidencialidad son manejados por el área de recursos humanos.
Contacto con las autoridades	NO	Las políticas propuestas son internas del área por lo que no se requiere contacto con proveedores de servicio de seguridad ejm: SNAP, Fiscalía, etc.
Contactos con grupos de interés especiales	SI	Se requiere contactos con organizaciones públicas o privadas especializados en seguridad de información para manejar y actualizar información sobre mejores prácticas de seguridad.
Revisión independiente de la seguridad de la información	NO	Las revisiones se realizarán periódicamente por todo el comité de seguridad dentro del área no por otros grupos ni personas independientemente.
Identificación de los riesgos relacionados con las partes externas	NO	Dentro del área del NOC no se manejan procesos en los que intervengan terceras partes directamente en políticas manejadas dentro del área.
Consideraciones de la seguridad cuando se trata con ciudadanos o clientes	SI	Se requiere manejar políticas de seguridad al manejarse información del área con los clientes o información de los clientes mismos.
Consideraciones de la seguridad en los acuerdos con terceras partes	NO	Los acuerdos con terceras partes lo maneja directamente el área de recursos humanos.
GESTIÓN DE LOS ACTIVOS		
Inventario de activos	SI	Se requiere inventariar todos los activos del área.
Responsable de los activos	SI	Se asigna un responsable de activos dentro del comité de seguridad de la información el cual se encargará de la administración de los activos dentro del área.
Uso aceptable de los activos	SI	Los servicios y aplicaciones deben de ser utilizados para fines del área.

Directrices de clasificación de la información	SI	La información es clasificada según su importancia dentro del área.
Etiquetado y manejo de la información	NO	No se requiere etiquetar la información ya que ésta es administrada y conocida únicamente por el área del NOC y sus clientes.
SEGURIDAD DE LOS RECURSOS HUMANOS		
Funciones y responsabilidades	NO	Todos los dominios respecto a seguridad de los recursos humanos son gestionados por parte del área de Recursos Humanos DEO dentro de la empresa.
Selección	NO	“
Términos y condiciones laborales	NO	“
Responsabilidades de la dirección a cargo del Funcionario	NO	“
Educación, formación y sensibilización en seguridad de la información	NO	“
Proceso disciplinario	NO	“
Responsabilidades de terminación del contrato	NO	“
Devolución de activos	NO	“
Retiro de los privilegios de acceso	NO	“
SEGURIDAD FISICA Y DEL ENTORNO		
Perímetro de la seguridad física	SI	Las políticas respecto a seguridad física y del entorno son gestionadas por parte del área de seguridad y vigilancia de la empresa. Respecto al perímetro utilizado para el funcionamiento del área debe de contar con seguridad física.
Controles de acceso físico	SI	Se deben de implementar los controles de acceso físico respectivos para poder ingresar al área.
Seguridad de oficinas, recintos e instalaciones	NO	Debido a la ubicación de las instalaciones y que se aplica control de acceso al área no se requiere implementar más controles físicos de seguridad.
Protección contra amenazas externas y ambientales	NO	Dentro del área no se utilizan materiales combustibles o peligrosos.
Trabajo en áreas seguras	NO	La compartición de la instalación con el área de Monitoreo de Red no permite

		utilizar un área catalogada como segura.
Áreas de carga, despacho y acceso público	NO	En el área no se gestiona despacho de material o equipos.
Ubicación y protección de los equipos	SI	Se deben de ubicar los equipos de manera que se restrinja su acceso a personal no autorizado.
Servicios de suministro	NO	Los servicios de suministro son gestionados por parte de la gerencia comercial.
Seguridad del cableado	SI	El cableado físico debe de ser instalado según normas de seguridad en donde se evite el acceso al cableado utilizado en el área.
Mantenimiento de los equipos	SI	Se deben de realizar mantenimientos a todos los equipos según las especificaciones técnicas.
Seguridad de los equipos fuera de las instalaciones	NO	Los equipos gestionados por los usuarios del área del NOC no son utilizados fuera del área.
Seguridad en la reutilización o eliminación de los Equipos	SI	Se debe de eliminar toda la información sensible en los equipos que se elimina y que no se van a utilizar dentro del área
Retiro de activos de la propiedad	SI	Se requiere autorización previa para retirar activos del área.
GESTIÓN DE COMUNICACIONES Y OPERACIONES		
Documentación de los procedimientos de Operación	SI	El área de SIS documentará información de ciertos procesos realizados dentro del área del NOC.
Gestión del Cambio	SI	Todo cambio realizado en el área debe de ser registrado para no causar interrupciones en el funcionamiento del área.
Distribución de funciones	NO	No se puede segmentar el área ya que todos los usuarios realizan las mismas funciones dentro del área asignada.
Separación de las instancias de Desarrollo, Pruebas, Capacitación y Producción	NO	Las gestiones de capacitación, pruebas y producción se desarrollan fuera del área del NOC dependiendo de la información que se maneje.
Presentación del Servicio	NO	Las funciones desempeñadas dentro del área no son gestionadas por terceros o

		grupos fuera del área sin previa autorización.
Monitoreo y revisión de los servicios, por terceros	NO	El área del NOC se encarga de monitorear y revisar los servicios que se brindan, estas funciones no son realizadas por terceros.
Gestión de los cambios en los servicios ofrecidos por terceros	NO	No se utilizan servicios ofrecidos por terceros dentro del área.
Gestión de la capacidad	NO	Este punto es gestionado directamente por el área de SIS garantizando la correcta funcionalidad de las herramientas, aplicativos y sistemas en general utilizados en el área del NOC.
Aceptación del Sistema	SI	Internamente se verifica el desempeño de los nuevos sistemas implementados en el área y de existir problemas en su funcionamiento se reporta al área de SIS para su verificación.
Controles contra código malicioso	SI	Se utilizará software autorizado únicamente por la empresa.
Controles contra códigos móviles	NO	No se gestiona redes móviles en el área del NOC.
Respaldo de la información	SI	La información sensible manejada dentro del área será respaldada internamente y por el área de SIS.
Controles de las redes	NO	No se puede segmentar la red buscando el uso exclusivo de la red para la operación.
Seguridad de los servicios de la red	SI	El uso de firewalls y antivirus dentro del área es requerido para el buen funcionamiento de los sistemas operativos.
Gestión de los medios removibles	NO	No se utilizan medios removibles dentro del área para gestión de los procesos internos.
Eliminación de los medios	NO	Actualmente el área no maneja información que vaya a ser eliminada especialmente en medios físicos.
Procedimientos para el manejo de la información	NO	No se requiere el etiquetado de medios de información en el área ya que únicamente personal del área tienen acceso a estos medios.

Seguridad de la documentación del sistema	SI	Los procesos de obtención de respaldo de la información del área del NOC deben realizarse bajo recomendaciones para resguardar dicha información y ofrecer seguridad en toda la gestión del proceso.
Políticas y procedimientos para el intercambio de Información	NO	Dentro del área del NOC no se intercambia información sensible con personas que no tengan autorización para gestionar dicha información.
Acuerdos para el intercambio	NO	Esta política no aplica ya que no se intercambia información sensible dentro del área.
Medios físicos en tránsito	NO	Dentro del área no se utilizan servicios de mensajería que utilicen medios físicos o personal dentro de la empresa.
Mensajería electrónica	NO	Los servicios de mensajería electrónica son utilizados únicamente para enviar información gestionada por el área.
Sistemas de información del negocio	NO	Dentro del área no se gestiona información financiera o administrativa, este proceso le compete a la gerencia comercial de la CNT.
Transacciones en línea	NO	En el área no se utilizan certificados con firmas electrónicas por parte de los usuarios.
Información disponible al público	NO	La información dentro del área es compartida únicamente con otras áreas competentes como mpls, dslam y los clientes directos del área.
Registros de auditorías	SI	Se requiere realizar registros de las funciones realizadas por los usuarios dentro del área.
Monitoreo de uso del sistema	NO	El registro de ingreso al sistema de todos los usuarios independientemente del área que labore lo gestiona el área de SIS.
Protección del registro de la información	NO	Las políticas de manejo de registros son gestionadas por el área de SIS incluyendo la protección de este proceso.
Registros del administrador y del operador	NO	El área directamente no lleva un registro de los procesos ya que no existen usuarios asignados

		como administradores dentro del área.
Registro de fallas	NO	Los errores en el sistema son reportados al área de SIS para su revisión y solución.
Sincronización de relojes	NO	Configuración manejada por el área de SIS, es importante mantener sincronizados todos los sistemas y aplicativos.
CONTROL DE ACCESO		
Política de control de acceso	SI	Solo personal autorizado tiene acceso a los sistemas de información.
Registro de usuarios	NO	El registro de acceso al sistema y ciertos aplicativos lo gestiona el área de SIS.
Gestión de privilegios	SI	Los privilegios otorgados a cada usuario son asignados dependiendo de la función que este cumple dentro del área.
Gestión de contraseñas para usuarios	SI	El uso de contraseñas para el ingreso a los sistemas informáticos por parte de los usuarios del NOC es primordial para la seguridad de información del área.
Revisión de los derechos de acceso de los usuarios	NO	Estas políticas son gestionadas por parte del área de SIS.
Uso de contraseñas	SI	El uso de contraseñas para el ingreso a los sistemas informáticos por parte de los usuarios del NOC es primordial para la seguridad de información del área.
Equipo de usuario desatendido	SI	Los equipos se bloquearán cuando no se utilizan en un cierto lapso de tiempo.
Política de puesto de trabajo despejado y pantalla Limpia	NO	Debido a que solo los usuarios del NOC utilizan los equipos informáticos dentro del área no se requiere utilizar estas políticas.
Política de uso de los servicios de red	NO	Estas políticas son gestionadas por el área de SIS.
Autenticación de usuarios para conexiones Externas	NO	Dentro del área del NOC no se realizan conexiones externas.
Identificación de los equipos en las redes	SI	Se requiere identificar los equipos a los que los usuarios acceden dentro de la red.
Protección de los puertos de	NO	En los equipos utilizados en los

configuración y diagnóstico remoto		enlaces todos los puertos están desbloqueados por defecto.
Separación en las redes	NO	No se requiere separar las redes dentro del área.
Control de conexión a las redes	NO	Estas políticas son gestionadas por el área de SIS.
Control del enrutamiento en la red	SI	Se requieren controles para gestionar el enrutamiento dentro de las redes.
Procedimiento de registro de inicio seguro	NO	Estas políticas son gestionadas por el área de SIS.
Identificación y autenticación de usuarios	NO	Estas políticas son gestionadas por el área de SIS.
Sistema de gestión de contraseñas	SI	Las contraseñas son secretas e intransferibles.
Uso de las utilidades del sistema	NO	Todos los aplicativos son administrados por el área de SIS.
Tiempo de inactividad de la sesión	NO	Esta política es reemplazada por el dominio de equipo de usuario desatendido.
Limitación del tiempo de conexión	NO	Estas políticas son gestionadas por el área de SIS.
Control de acceso a las aplicaciones y a la Información	SI	Cada funcionario del NOC utiliza su usuario y clave de acceso a las aplicaciones y utilitarios para evitar el mal uso de la información interna.
Restricción de acceso a la información	SI	La información del área es manejada únicamente por personal autorizado.
Aislamiento de sistemas sensibles	NO	Dentro del área no se utilizan sistemas sensibles o utilizados en un entorno compartido.
Computación y comunicaciones móviles	NO	No se utilizan comunicaciones móviles en la gestión del área del NOC.
Trabajo remoto	NO	Todas las gestiones son utilizadas directamente, no se utilizan accesos remotos.
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN		
Análisis y especificaciones de los requerimientos de Seguridad	NO	Este dominio es gestionado por el área de sistemas SIS de la empresa.
Validación de datos de entrada	NO	“
Control de procesamiento interno	NO	“

Integridad del mensaje	NO	“
Validación de datos de salidas	NO	“
Política sobre el uso de controles criptográficos	NO	“
Gestión de claves	NO	“
Control del software operativo	SI	Se requiere minimizar el cambio en los sistemas al implementar nuevos software.
Protección de los datos de prueba del sistema	NO	Este dominio es gestionado por el área de sistemas SIS de la empresa
Control de acceso al código fuente de los programas	NO	“
Procedimiento de control de cambios	SI	Todo cambio debe de ser autorizado y realizado por personal autorizado.
Revisión técnica de las aplicaciones después de los cambios en el sistema operativo	NO	Este dominio es gestionado por el área de sistemas SIS de la empresa.
Restricción del cambio de paquetes de software	NO	Este dominio es gestionado por el área de sistemas SIS de la empresa.
Fuga de información	SI	Todos los medios y comunicaciones deben de ser revisados para evitar fuga de información.
Desarrollo de software contratado externamente	NO	Este dominio es gestionado por el área de sistemas SIS de la empresa.
Control de las vulnerabilidades técnicas	NO	“
GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN		
Reporte sobre los eventos de seguridad de la Información	SI	Se manejan procedimientos internos del área para el manejo de incidentes.
Reporte sobre las debilidades en la seguridad	SI	De cada proceso gestionado se realiza un análisis de los problemas recurrentes.
Responsabilidades y procedimientos	NO	Cada usuario maneja un incidente diferente y es responsable de su cierre.
Aprendizaje debido a los incidentes de seguridad de la información	SI	Análisis general de todos los casos revisados internamente.
Recolección de evidencias	NO	No se manejan políticas concernientes a evidencias encontradas.
GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		
Inclusión de la seguridad de la información en el proceso de gestión de la	SI	Es primordial el análisis de la seguridad para la continuidad del negocio.

continuidad del negocio		
Continuidad del negocio y evaluación de riesgos	NO	Dominios manejados por el área de SIS.
Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información	NO	“
Estructura para la planificación de la continuidad del negocio	SI	Se maneja SLA’s con los clientes y proveedores de servicios que tienen relación con el área del NOC.
Pruebas, mantenimiento y revisión de los planes de continuidad del negocio	NO	Dominios manejados por el área de SIS.
CUMPLIMIENTO		
Identificación de la legislación aplicable	NO	Dominios manejados por el área de SIS.
Derechos de Propiedad Intelectual	SI	Se debe de utilizar únicamente software garantizado por proveedores con derechos de propiedad intelectual.
Protección de registros en cada entidad	NO	Dominios manejados por el área de SIS.
Protección de los datos y privacidad de la información personal	NO	“
Prevención del uso inadecuado de servicios de procesamiento de información	NO	“
Reglamentación de controles criptográficos	NO	“
Cumplimiento con las políticas y las normas de la Seguridad	SI	El comité de seguridad seleccionado debe de velar por el cumplimiento de las normas y políticas propuestas para el buen desempeño del SGSI diseñado.
Verificación del cumplimiento técnico	NO	Dominios manejados por el área de SIS.
Controles de auditoría de los sistemas de Información	NO	“
Protección de las herramientas de auditoría de los sistemas de información	NO	“

Las principales políticas aplicadas para el desarrollo del SGSI se detallan a continuación:

3.3.2 Política de Seguridad de la Información

3.3.2.1 Situación Actual

La CNT utiliza políticas de seguridad de la información que contempla normativas sobre la correcta administración de la información, en forma general estas normativas se aplican a todas las áreas y todos los colaboradores de la empresa.

3.3.2.2 Situación Propuesta

Siendo el NOC un área crítica por la información que se maneja internamente, las funciones desempeñadas dentro de la empresa y basados en la política actualmente aplicada directamente al NOC; se busca diseñar una nueva política de seguridad de la información que pueda ser utilizada exclusivamente por el área del NOC, ésta política será diseña conforme a las funciones que cumple el NOC dentro de la empresa y las funciones desempeñadas por cada usuario dentro del área.

3.3.2.3 Situación Ideal

Crear un documento que contenga políticas de seguridad de la información el cual estará disponible por la gerencia del área en el caso de analizar una posible implementación del SGSI propuesto.

3.3.3 Organización de la Seguridad de la Información

3.3.3.1 Situación Actual

Internamente en el área del NOC no se dispone de un grupo organizacional que administre las políticas actualmente utilizadas en la empresa y que sean aplicadas directamente al área.

Actualmente la empresa maneja políticas de seguridad con todos sus empleados manejando acuerdos de confidencialidad, estos acuerdos se firman personalmente por cada empleado de la empresa al ingresar a funciones o ser contratados, este registro se lo realiza en documentos físicos los mismos que son administrados por la gerencia de recursos humanos.

3.3.3.2 Situación Propuesta

Se requiere seleccionar personal organizacional que administre y gestione el SGSI propuesto, este grupo organizacional gestionará las políticas internas que se utilizarán dentro del área del NOC.

3.3.3.3 Situación Ideal

Se designará un comité de gestión de seguridad de la información el cual lo conformará los cargos directivos del área, este comité tendrá como principal función el manejo y coordinación del SGSI definiendo y manteniendo las políticas diseñadas, este comité entrará en función en el caso que el SGSI se implemente.

Se deberá identificar y evaluar los riesgos para la información y los servicios de procesamiento de información del área.

3.3.4 Gestión de los Activos

3.3.4.1 Situación Actual

Actualmente en el área se abarcan las normas de seguridad en la gestión de activos tales como el control de acceso y el uso de ciertos recursos del área.

3.3.4.2 Situación Propuesta

Se recomienda tener un inventario conformado por activos de software y hardware categorizando la información que el área maneja como el activo más importante. Los activos pueden ser clasificados y etiquetados de acuerdo a su tipo y funcionalidad dentro del área.

3.3.4.3 Situación Ideal

El inventario contendrá todos los activos del área entre estos la documentación manejada, hardware, software, activos de soporte de redes y activos de estructura organizacional, la información de los activos se la debe de almacenar en formatos físicos y electrónicos.

Se asignará una persona o un grupo de personas responsable de los activos identificados en el área de manera que administre el inventario descrito.

Es necesario identificar, documentar e implementar las reglas sobre el uso aceptable de los activos asociados con los servicios de procesamiento de la información.

Los servicios de correo e internet deben utilizarse exclusivamente para las tareas propias de las funciones que se desarrollan en el área y no debe utilizarse para ningún otro fin.

La información debe de ser clasificada y etiquetada en términos de su valor y la importancia para el área, la misma puede ser clasificada en información pública o confidencial.

3.3.5 Seguridad de los Recursos Humanos

3.3.5.1 Situación Actual

Las políticas de seguridad de recursos humanos son manejadas y administradas por el área de Recursos Humanos (DEO) dentro de la empresa CNT en general; se utilizan las mismas políticas para todos los empleados nuevos y antiguos al ingresar y desvincularse a la empresa independientemente del área donde desempeñe sus funciones.

3.3.6 Seguridad Física y del Entorno

3.3.6.1 Situación Actual

La ubicación física del área del NOC se encuentra en el edificio Doral que es la sucursal principal de la empresa en la ciudad de Quito.

El área se encuentra ubicada en el segundo piso del edificio, existe un primer filtro de seguridad en la entrada principal del edificio el cual está custodiado por personal de vigilancia de la empresa los cuales tienen como disposición verificar las credenciales de todo el personal que ingresa al edificio.

Al ingresar al segundo piso del edificio existe otro filtro de seguridad el cual se ubica en las gradas de acceso, personal de vigilancia verifica nuevamente la credencial de cada persona que ingresa al piso y realiza una revisión de los objetos personales que lleva la persona.

Existe un tercer filtro de seguridad que es el acceso biométrico al área, este acceso se utiliza para registro de personal pero no para autorización de ingreso al área.

La administración de la seguridad física y del entorno en la infraestructura de todas las sucursales de la empresa a nivel provincial actualmente es gestionada por la gerencia de finanzas y administración de la CNT directamente por el área de seguridad y vigilancia.

3.3.6.2 Situación Propuesta

Seguridad en el perímetro del área, controles de acceso físico, protección y mantenimiento de los equipos, seguridad del cableado y retiro de activos de la propiedad.

3.3.6.3 Situación Ideal

Las políticas de seguridad física y del entorno propuestas serán aplicadas únicamente al área del NOC y serán gestionadas por el comité de seguridad de la información asignado dentro del área.

3.3.7 Gestión de Comunicaciones y Operaciones

3.3.7.1 Situación Actual

En el área del NOC no se documenta el procesamiento y manejo de la información utilizada. Toda la información es documentada y respaldada por parte del área de sistemas SIS de la empresa.

El área de sistemas SIS aplica en el área del NOC políticas de seguridad para prevenir daños por uso de código malicioso y uso incorrecto del sistema; en

donde se aplican políticas para la identificación y registro de las personas que acceden a las herramientas y utilitarios del área.

3.3.7.2 Situación Propuesta

Establecer políticas que administran la documentación y registro de los procesos realizados en el NOC así como los cambios realizados en ellos.
Se analizarán políticas de seguridad relacionadas con las características y uso de los sistemas y redes de datos utilizadas dentro del área.

3.3.7.3 Situación Ideal

Las políticas de seguridad serán gestionadas por el comité de seguridad asignado dentro del área, ciertas políticas son manejadas directamente por el área de sistemas SIS pero se proponen políticas para el manejo de información, procesos y sistemas que se utilizan dentro del área y que incluyen políticas de control, documentación y administración.

3.3.8 Control de Acceso

3.3.8.1 Situación Actual

En el área del NOC actualmente se manejan políticas de seguridad que gestionan el acceso a los recursos, herramientas y aplicativos utilizados internamente, éstas políticas son gestionadas en algunos casos por otras áreas involucradas en la gestión interna del área del NOC dependiendo del uso de las herramientas por parte de los usuarios, por ejemplo: el área de MPLS gestiona los privilegios y el acceso a la red MPLS para la revisión del enrutamiento de los enlaces y el área de DSLAM gestiona el acceso y privilegios para el uso de las herramientas para la verificación del estado y características de puertos en enlaces ADSL.

Las políticas de seguridad respecto al acceso a la red y a los diferentes gestores utilizados en el área del NOC son gestionadas por parte del área de sistemas SIS, en éstas políticas se gestionan los privilegios de uso para los usuarios, registro, control de acceso y uso de contraseñas.

3.3.9 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

3.3.9.1 Situación Actual

Las políticas de seguridad de la información de los sistemas de información entre ellos los sistemas operativos, aplicaciones utilizadas en el área y servicios utilizados por los usuarios son gestionadas por el área de sistemas SIS de la empresa.

3.3.10 Gestión de los Incidentes de la Seguridad de la Información

3.3.10.1 Situación Actual

El área del NOC utiliza los siguientes procedimientos para la gestión de incidencias dentro del área, para esta gestión utiliza la herramienta Remedy, éste gestor se utiliza para aperturar, dar seguimiento, resolver y cerrar las incidencias reportadas por los clientes.

El cliente reporta el caso vía telefónica o por correo electrónico, esta información es manejada por el área de N0 dentro del área del NOC, los Analistas N0 de Soporte Corporativo y Gubernamental validan la información del cliente utilizando los datos registrados del mismo en el sistema con los indicados por el cliente al reportar el caso.

Se apertura una incidencia en el gestor Remedy agregando la información indicada por el cliente y la validada en el sistema, es muy importante tener como dato para la búsqueda el número de servicio o piloto del cliente.

La incidencia es asignada a un Analista de Nivel 1 N1 de Soporte Corporativo y Gubernamental para dar seguimiento del caso, averiguar el problema, buscar la causa y su posible solución, en esta etapa la incidencia puede tardar horas e incluso días sin encontrar una solución para poder proceder con la resolución y cierre del caso.

Existen casos en que la incidencia es escalada a otra área fuera del N1 para poder gestionar su seguimiento y posible solución, por ejemplo:

- Cuando se requiere la revisión de personal de última milla en sitio se escala el caso al área y provincia correspondiente.
- Cuando se solicita por parte del cliente configuraciones en los equipos o cambios en el enrutamiento de su enlace se escala al área de Nivel 2 N2 para que sus analistas procedan con el requerimiento.

Después de realizar estos cambios se confirma con el área de N1 para poder proceder con el cierre de la incidencia.

3.3.11 Gestión de la Continuidad del Negocio

3.3.11.1 Situación Actual

El área del NOC actualmente no utiliza políticas de seguridad que permitan reaccionar frente a la interrupción de las actividades del área y protección de los procesos críticos que el área maneja frente a desastres o grandes fallos del sistema de información.

3.3.11.2 Situación Propuesta

Se utilizará políticas de seguridad de la información que garanticen la continuidad de la gestión del área del NOC en todas sus funciones y de todas las herramientas que los usuarios del área utilizan.

3.3.11.3 Situación Ideal

La continuidad del negocio es gestionada por el responsable del área de tecnologías, es la persona encargada de administrar las políticas de seguridad de la información para garantizar la continuidad de las funciones del área frente a eventos fortuitos y fallos en el sistema.

Se manejarán acuerdos de nivel de servicio SLA`s con los clientes cuando los enlaces reportados como caídos tardan demasiado tiempo en ser gestionados,

estos acuerdos son administrados y manejados por el área comercial conjuntamente con el cliente.

3.3.12 Cumplimiento

3.3.12.1 Situación Actual

Las políticas de seguridad en este punto contempla el cumplimiento de la ley, estatutos, normativas y regulación establecida dentro de la empresa CNT a nivel nacional, éstas políticas se aplican a todas las áreas y personal que labora en la empresa y son gestionadas por la Gerencia Nacional Jurídica.

4. Capítulo IV. Evaluación del Sistema de Gestión de Seguridad de la Información

4.1 Análisis de las Soluciones Propuestas del SGSI Diseñado

En base a las políticas y dominios de seguridad de la información recomendadas en el esquema gubernamental de seguridad de la información para el diseño de sistemas de gestión de seguridad de la información en entidades públicas y tomando como referencia las políticas propuestas se analizará las diferentes recomendaciones y posibles soluciones a los problemas encontrados dentro del área en lo que concierne a seguridad de la información (Anexo 4).

4.1.1 Política de Seguridad de la Información

El documento creado que contiene las políticas propuestas de seguridad de la información y sobre el cual se gestionará el SGSI diseñado para el NOC será administrado por el comité seleccionado de seguridad de la información, se propone que este documento lleve el nombre de “Sistema de Gestión de Seguridad de la Información SGSI-NOC”.

- El documento es administrado por el comité de seguridad de la información, utilizado por todo el personal del área y en el caso de requerir su implementación se necesita la aprobación de los directivos del área.

- Se requiere realizar revisiones periódicas del documento y las políticas utilizadas en el SGSI propuesto, estas revisiones también se las realizará cuando haya cambios significativos.

- Este documento definirá procesos, procedimientos y tecnologías que garanticen la confidencialidad, integridad y disponibilidad de la información que se maneja en el área.

- Se debe de realizar revisiones anuales de la política de seguridad de la información en el caso que sea implementado el SGSI propuesto para el uso interno en el área.

4.1.2 Organización de la Seguridad de la Información

Los infringimientos en la política de seguridad de la información propuesta para aplicarse dentro del área del NOC se reportarán directamente a los dos coordinadores asignados dentro del comité de gestión de seguridad de la información, dependiendo del infringimiento y la clase de activo que pueda ser afectado se realizará el seguimiento requerido por parte del oficial de seguridad de la información.

4.1.2.1 Comité de Seguridad de la Información

El comité de gestión de seguridad de la información en el área del NOC está conformado por directivos del área. Dicho comité tiene como principales funciones gestionar el cumplimiento de las políticas utilizadas en el SGSI propuesto, adicional a esto gestionará y monitoreará la aplicación de la norma INEN-ISO/IEC 27001 en el SGSI propuesto y sus políticas de gestión de seguridad de la información. Dentro del comité se nombrará un oficial de seguridad de la información y un responsable de seguridad del área de tecnologías de la información que se encargarán de definir procedimientos para el control de cambios a los procesos operativos, definir procedimientos para el manejo de incidentes de seguridad, verificar el cumplimiento de las normas, controlar la existencia de documentación física o electrónica relacionada con los procedimientos, etc.

Figura 24. Estructura del Comité de Gestión de Seguridad de la Información en el Área del NOC

El personal del área del NOC se manejará con la misma política en lo que compete a registros de acuerdos de confidencialidad. Cada nuevo usuario del área firmará un acuerdo en un documento físico administrado por el área de recursos humanos.

Se establecerá procedimientos que especifiquen cuándo y a cuáles autoridades se reportarán incidentes derivados del infringimiento de la política de seguridad.

El área del NOC está bajo la supervisión del área de sistemas SIS de la empresa CNT en lo que concierne a capacitar a los usuarios dentro del área en temas de seguridad de la información, analizar mejores prácticas y estar constantemente actualizado de información pertinente a gestión de la seguridad.

Tabla 6. Comité de Seguridad

COMITÉ DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DEL NOC			
CARGO	**PERSONA ASIGNADA**	**ROL DESEMPEÑADO**	**FUNCIÓN**
GERENTE DEL ÁREA DE SOPORTE CORPORATIVO Y GUBERNAMENTAL	ING. OSCAR CORREA	DIRECTOR ADMINISTRATIVO	GESTIONARÁ EL ENTREGABLE DEL DOCUMENTO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.
JEFE DEL ÁREA DE SOPORTE CORPORATIVO Y GUBERNAMENTAL	INGA. MERY ALARCÓN	COORDINADOR	LA COORDINACIÓN ESTARÁ A CARGO DEL COMITÉ DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.
SUPERVISOR ENCARGADO N2	ING. ANDRÉS SALAZAR	OFICIAL DE SEGURIDAD DE LA INFORMACIÓN	SERÁ EL RESPONSABLE DE COORDINAR LAS ACCIONES DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Y DE IMPULSAR LA IMPLEMENTACIÓN Y CUMPLIMIENTO DEL SGSI.
SUPERVISOR ENCARGADO N0 - N1	ING. JORGE BUENO	RESONSABLE DE RECURSOS HUMANOS	CUMPLIRÁ LA FUNCIÓN DE COMUNICAR A TODO EL PERSONAL QUE INGRESA, DE SUS OBLIGACIONES RESPECTO DEL CUMPLIMIENTO DEL SGSI Y DE TODAS LAS NORMAS, PROCEDIMIENTOS Y PRÁCTICAS QUE DE ÉL SURJAN.

ANALISTA DE SEGUIMIENTO N0 – N1	ING. JORGE JARA	RESPONSABLE DEL ÁREA DE TECNOLOGÍAS	CUMPLIRÁ LA FUNCIÓN DE CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD INFORMÁTICA ESTABLECIDOS PARA LA OPERACIÓN, ADMINISTRACIÓN Y COMUNICACIÓN DE LOS SISTEMAS Y RECURSOS DE TECNOLOGÍA DEL ÁREA.
ANALISTA DE SEGUIMIENTO N0 – N1	ING. JORGE TOBAR	RESPONSABLE DE ACTIVOS	ELABORAR EL INVENTARIO DE LOS ACTIVOS A SU CARGO Y MANTENERLO ACTUALIZADO. CLASIFICAR, DOCUMENTAR Y MANTENER ACTUALIZADA LA INFORMACIÓN Y LOS ACTIVOS, Y DEFINIR LOS PERMISOS DE ACCESO A LA INFORMACIÓN.
ANALISTA DE SEGUIMIENTO N0 – N1	ING. EDGAR ALARCÓN	RESPONSABLE DE AUDITORÍA INTERNA	VERIFICARÁ EL CUMPLIMIENTO DEL SGSI EN LA GESTIÓN DE TODOS LOS CONTRATOS, ACUERDOS U OTRA DOCUMENTACIÓN DE LA INSTITUCIÓN CON SUS EMPLEADOS Y CON TERCEROS.

4.1.2.1.1 Matriz RACI

Esta matriz se utiliza para asignar roles o responsabilidades a las personas que conforman el comité (Tabla 7).

Rol			Descripción
R	*Responsible*	Responsable	Este rol corresponde a quien efectivamente realiza la tarea. Lo más habitual es que exista sólo un encargado (R) por cada tarea; si existe más de uno, entonces el trabajo debería ser subdividido a un nivel más bajo, usando para ello las matrices RASCI.
A	*Accountable*	Quien rinde cuentas	Este rol se responsabiliza de que la tarea se realice y es el que debe rendir cuentas sobre su ejecución. Sólo puede existir una persona que deba rendir cuentas (A) de que la tarea sea ejecutada por su responsable (R).
C	*Consulted*	Consultado	Este rol posee alguna información o capacidad necesaria para realizar la tarea.
I	*Informed*	Informado	Este rol debe ser informado sobre el avance y los resultados de la ejecución de la tarea. A diferencia del consultado (C), la comunicación es unidireccional.

Figura 25. Roles en la matriz RACI

Tabla 7. Matriz RACI del Comité de Seguridad

RESPONSABLE / *TAREA*	DIRECTOR ADMINISTRATIVO	COORDINADOR	OFICIAL DE SEGURIDAD DE LA INFORMACIÓN	RESONSABLE DE RECURSOS HUMANOS	RESPONSABLE DEL ÁREA DE TECNOLOGÍAS	RESPONSABLE DE ACTIVOS	RESPONSABLE DE AUDITORÍA INTERNA
Gestión del documento	R	A	A	C	C	C	I
Gestión del comité	A	R	A	C	C	C	I
Coordinación del comité	A	R	R	I	C	C	I
Implementación del SGSI	R	C	A	C	C	C	I
Comunicar información	C	C	A	R	C	C	R
Gestión de sistemas y recursos tecnológicos	C	C	C	I	R	A	I
Gestionar el inventario	C	C	C	I	A	R	I
Verificar el SGSI	C	R	R	I	C	C	I

En la Tabla No. 5 se describe los roles, funciones y responsabilidades de los directivos seleccionados que conforman el comité según tareas específicas que se realizan dentro del comité.

Estos roles son asignados de acuerdo al cargo y jerarquía del directivo seleccionado dentro del comité.

El oficial de seguridad de la información tendrá como una de sus principales funciones convocar al comité de seguridad de la información regularmente o cuando la situación lo amerite.

4.1.2.2 Metodología de Análisis y Gestión de Riesgos

En el cuadro de valoración de activos, los mismos serán clasificados según el riesgo y la característica del activo como la disponibilidad (D), integridad (I) y confidencialidad (C).

A continuación en la Tabla 8 se detalla la valoración de los activos del área del NOC:

Tabla 8. Valoración de Activos del Área del NOC

CANTIDAD	DESCRIPCIÓN	VALOR			VALOR ACUMULADO
		D	I	C	
-	DATOS	-	-	-	-
-	GESTIÓN DE REDES	5	5	5	5
-	SOPORTE DE REDES	5	-	5	5
-	SERVICIO DE INTERNET	5	-	5	5
-	SERVICIO DE DATOS	5	-	5	5
-	SERVICIO DE CORREO	5	-	5	5
-	MICROSOFT WINDOWS	5	-	-	5
-	OPEN FLEXIS	4	-	-	4
-	ZOC	5	-	-	5

-	MICROSOFT EXCHANGE	5	-	-	5
-	AVAYA	5	-	-	5
-	REMEDY	5	5	5	5
-	ANTIVIRUS AVG	5	-	-	5
-	FIREFOX	4	-	-	4
1	CONVERSOR TP-LINK WDM 10/100MBPS	5	-	-	5
1	ROUTER CISCO 800	5	-	-	5
3	SWITCH D-LINK 16 PUERTOS	5	-	-	5
20	COMPUTADOR INTEL CORE	5	-	-	5
-	SOPORTES DE INFORMACIÓN	-	-	-	-
1	1 PANTALLA LCD DE 50”	5	-	-	5
1	1 IMPRESORA LÁSER	4	-	-	4
-	RED LOCAL	5	5	5	5
-	WIRELESS INVITADOS	5	-	-	5
-	WIRELESS MÓVILES	5	-	-	5
-	WIRELESS USUARIOS	5	-	-	5
-	RED DE INTERNET	5	5	5	5
-	INSTALACIONES	-	-	-	-

-	PERSONAL	-	-	-	-

Se aplican los valores calificativos de 5 para los activos más importantes que maneja la entidad y se califica con valor de 1 aquellos activos que no provocan perjuicio para la entidad en el caso de producirse una falla.

Existen casos en que las características sean estas disponibilidad, integridad y confidencialidad no aplica calificación ya que depende de la función o el uso del activo de la empresa por lo que se asigna valor nulo.

4.1.2.2.1 Determinación del Riesgo

El riesgo es la medida del daño probable sobre un sistema. A continuación en la Tabla 9 se muestra la determinación del riesgo sobre los activos de la entidad tomando en cuenta las características de cada activo como son la disponibilidad (D), integridad (I) y confidencialidad (C) y las amenazas a las que están expuestos los activos.

Tabla 9. Determinación del Riesgo Dentro del Área del NOC

ACTIVO \ AMENAZA	**SERVICIOS**			**DATOS**			**APLICACIONES**			**EQUIPOS INFORMATICOS**			**SOPORTE DE INFORMACION**			**EQUIPAMIENTO AUXILIAR**			**INSTALACIONES**			**PERSONAL**		
DESCRIPCION	**D**	**I**	**C**	**D**	**I**	**C**	**D**	**I**	**C**	**D**	**I**	**C**	**D**	**I**	**C**	**D**	**I**	**C**	**D**	**I**	**C**	**D**	**I**	**C**
ORIGEN NATURAL																								
Fuego										X			X			X			X					
Daño por Agua										X			X			X			X					
Desastres Naturales										X			X			X			X					
ORIGEN INDUSTRIAL																								

Fuego				X	X	X	X	
Daño por Agua				X	X	X	X	
Contaminación Mecánica				X	X	X	X	
Contaminación Electromagnética				X	X	X	X	
Avería de Origen Físico o Lógico				X	X	X	X	
Corte de Suministro Eléctrico				X	X	X	X	X
Condiciones Inadecuadas de Temperatura/Humedad				X	X	X	X	X
Interrupción de Otros Servicios y Suministros Esenciales				X	X	X	X	X
Degradación de los Soportes de Almacenamiento				X	X	X	X	
Emanaciones Electromagnéticas				X	X	X	X	
Desastres Industriales				X	X	X	X	X
ORIGEN/ERRORES								
Errores de los Usuarios	X	XXX	X	X	X	X	X	
Errores del Administrador	X	XXX	XX	X	X	X	X	
Errores de Monitoreo	X	XX	XX	X	X	X	X	
Errores de Configuración	XX	XXX	XX	X	X	X	X	

Deficiencias de la Organización	XXX	XXX	XXX	X	X	X	X	
Difusión de Software Dañino	XXX	XXX	XXX	X	X	X	X	
Errores de Encaminamiento	X	XX	X					
Errores de Secuencia	X	X	X					
Escapes de Información	XX	XXX	XX					
Alteración de la Información	XXX	XXX	XX					
Introducción de Información Incorrecta	XXX	XXX	XX					
Degradación de la Información	X	X	X					
Destrucción de Información	XXX	XXX	XX					
Divulgación de Información	XXX	XXX	XX					
Vulnerabilidades de los Programas	XX	XXX	XX					
Errores de Mantenimiento/Actualización de Programas	XX	XX	XX					
Errores de Mantenimiento/Actualización de Equipos	XX	XX	XX	XX	XX	XX	XX	
Caída del Sistema por Agotamiento de Recursos	X	X	X	X	X	X	X	
Indisponibilidad del	XX	XX	XX	X	X	X	X	X

Personal								
ORIGEN/ATAQUES								
Manipulación de la Información	XX	XXX	XX					
Suplantación de la Identidad del Usuario	XX	XXX	XX	X	X	X	X	XX
Abuso de Privilegios de Acceso	XX	XXX	XX	X	X	X	X	XX
Uso no Previsto	X	X	X	X	X	X	X	X
Difusión de Software Dañino	XX	XXX	XX	X	X	X	X	
Reencaminamiento de mensajes	X	XXX	XX					
Alteración de Secuencia	X	XX	XX					
Acceso no Autorizado	XX	XXX	XX	X	X	X	X	XXX
Interceptación de Información	XX	XXX	XX					XXX
Modificación de la Información	XX	XXX	XX					XXX
Introducción de Falsa Información	XX	XXX	XX					XXX
Corrupción de la Información	XX	XXX	XX					XXX
Destrucción de la Información	XXX	XXX	XX					XXX
Divulgación de Información	XXX	XXX	XX					XXX
Manipulación de	XX	XXX	XX	X	X	X	X	

Programas								
Denegación de Servicio	XX	XXX	XX	X	X	X	X	XX
Robo	XXX	XXX	XX	X	X	X	X	XXX
Ataque Destructivo	XXX	XXX	XXX	XX	XX	XX	XX	XXX
Ocupación Enemiga	XXX	XXX	XX	XX	XX	XX	XX	XXX
Indisponibilidad del Personal	X	X	X	X	X	X	X	X
Extorción	XX	XXX	XX	X	X	X	X	XXX
Ingeniería Social	XXX	XXX	XXX	X	X	X	X	XXX

4.1.2.3 Políticas Diseñadas de Acceso a la Información:

- El personal del área del NOC tiene solo acceso a la información disponible para el uso dentro del área y las funciones determinadas de cada usuario dentro de la misma.

- El acceso a la información por personas fuera del área debe de ser documentado y autorizado por la persona encargada de la administración de la información solicitada.

- Los privilegios otorgados a los usuarios del área deben de ser regulados por el personal del área de sistemas de la empresa, estos privilegios son asignados de acuerdo a la función desempeñada por el usuario, estos privilegios será eliminados según las condiciones actuales del usuario. En el caso de que la persona cambie de área los privilegios serán otorgados o retirados según la nueva función a desempeñar y cuando el funcionario sea retirado de la empresa por culminación de contrato todos los privilegios son retirados definitivamente.

- Se debe de tener un registro de todos los eventos ocurridos dentro del área respecto acceso a la información y acceso a los recursos y aplicaciones utilizadas dentro del área.

4.1.2.4 Políticas Diseñadas de Administración de Cambios:

- Toda modificación en los programas, utilitarios y herramientas de uso dentro del área debe de ser solicitada por la persona que desea realizar dicho cambio y esta solicitud debe de ser aprobada por la persona responsable de administrar ese recurso.

- Bajo ninguna circunstancia un cambio puede ser aprobado, realizado o implementado por la misma persona o área que pretende realizar el cambio.

- Todo cambio debe de ser documentado desde su solicitud hasta su implementación.

- Todo cambio debe de realizarse bajo condiciones específicas de manera que no disminuya la seguridad de la información existente en el área.

Se requiere mantener contacto con organizaciones públicas y privadas especializadas en seguridad de la información para mantener actualizada la información y mejorar los conocimientos concernientes a la gestión de la seguridad.

En el área del NOC se recomienda realizar revisiones independientes y periódicas del sistema de gestión de seguridad de la información, adicional a esto se deben de realizar revisiones cada que haya cambios significativos dentro del área sean estos técnicos o administrativos.

4.1.3 Gestión de los Activos

Se dispondrá de un inventario de activos el cual nos permite clasificar a los activos según su funcionalidad.

4.1.3.1 Control de Activos

En este caso se deben de valorar los activos que la empresa maneja. Todos los activos serán administrados por el responsable de activos asignado en el comité de gestión de seguridad de la información.

4.1.3.1.1 Valoración de Datos

Actualmente en el área no se disponen de bases de datos o sistemas integrados que puedan utilizarse para almacenar información que sea utilizada dentro del área, todas las bases de datos de todas las áreas que conforman la empresa son administradas por el área de sistemas SIS de la empresa.

4.1.3.1.2 Valoración de Servicios

Actualmente en el área se brindan los siguientes servicios:

- Gestión de Redes.
- Soporte de Redes.
- Servicio de Internet.
- Servicio de Datos.
- Servicio de Correo.

4.1.3.1.3 Valoración de Aplicaciones

Actualmente en el área se utilizan las siguientes aplicaciones:

- Microsoft Windows.
- Open Flexis.
- ZOC.
- CACTI.
- Microsoft Exchange.
- Avaya.
- Remedy.
- Antivirus AVG.
- Firefox.

4.1.3.1.4 Valoración de Equipos Informáticos

Actualmente en el área se utilizan los siguientes equipos informáticos:

Tabla 10. Equipos de Red del Área del NOC

DESCRIPCIÓN	**CANTIDAD**	**ESTADO**
CONVERSOR TP-Link WDM 10/100Mbps	1	ACTIVO
ROUTER CISCO 800	1	ACTIVO
SWITCH D-Link 16 PUERTOS	3	ACTIVO
COMPUTADOR INTEL CORE	20	ACTIVO

4.1.3.1.5 Valoración de Soportes de Información

Actualmente en el área no existen equipos que sean gestionados por personal del área del NOC en los cuales se pueda respaldar la información utilizada dentro del área, los equipos utilizados para dicha función son gestionados por el área de sistemas SIS de la empresa.

4.1.3.1.6 Valoración de Equipamiento Auxiliar

Actualmente en el área se utilizan los siguientes equipos auxiliares:

- 1 Pantalla LCD de 50” para monitoreo de la red.
- 1 Impresora Láser para uso interno de personal del área.

4.1.3.1.7 Valoración de Redes de Comunicaciones

Actualmente en el área se utilizan las siguientes redes de comunicación:

Tabla 11. Redes de Comunicación del Área del NOC

DESCRIPCIÓN	SUBRED
RED LOCAL	10.10.5.0/24
WIRELESS INVITADOS	10.10.6.0/24
WIRELESS MÓVILES	10.10.7.0/24
WIRELESS USUARIOS	10.10.8.0/24
RED DE INTERNET	192.168.10.30/29

4.1.3.1.8 Valoración de Instalaciones

Actualmente todo el personal del área labora en un espacio de 20*30 metros ubicado en el segundo piso del edificio Doral en el extremo nororiente del edificio.

4.1.3.1.9 Valoración de Personal

Actualmente dentro del área existen los siguientes cargos y funcionalidades:

- Jefe del Área de Soporte Corporativo y Gubernamental.
- Supervisor Encargado N2.
- Supervisor Encargado N0 - N1.
- Analista de Seguimiento N0 – N1.
- Analista N0 de Soporte Corporativo y Gubernamental.
- Analista N1 de Soporte Corporativo y Gubernamental.
- Analista N2 de Soporte Corporativo y Gubernamental.

4.1.3.2 Políticas Diseñadas de Administración de la Seguridad:

- Se debe de realizar el análisis de riesgos de forma periódica, se recomienda una vez al año.

- Respecto a mala utilización de los recursos informáticos dentro del área o sospecha de uso mal intencionado de los mismos, se debe de reportar

inmediatamente por la persona que lo detecta a los coordinadores asignados en el comité de seguridad de la información.

- El comité de seguridad de la información asignado dentro del área es el grupo encargado de divulgar información o capacitar al resto del personal que desconoce la gestión de la seguridad de la información dentro del área.

4.1.3.3 Información Utilizada Dentro del Área del NOC

Como se mencionó anteriormente la función del NOC dentro de la empresa es manejar los enlaces de internet y datos de clientes corporativos y gubernamentales a nivel nacional por ende toda la información maneja de los clientes que tienen servicio con la empresa es clasificada como confidencial y de uso exclusivo dentro del área.

Los servicios de correo electrónico institucional e internet deben utilizarse para las funciones específicas del área y no deben utilizarse para ningún otro fin.

4.1.4 Seguridad de los Recursos Humanos

Los procedimientos de selección de personal que ingrese o se desvincule del área del NOC dentro de la empresa son administrados por el área de Recursos Humanos DEO, ésta administración incluye gestión sobre los procesos, documentación y personal de las áreas competentes.

4.1.4.1 Políticas Diseñadas de Seguridad para Terceras Personas:

- Los recursos informáticos que no sean administrados por el área y que sean utilizados dentro del área por terceras personas deben de ser legalizados para su utilización y se debe de documentar un acuerdo de ambas partes.

- Se debe de firmar acuerdos de confidencialidad en el caso de que algún usuario ajeno al área requiera utilizar recursos dentro del área.

- Las conexiones de equipos, sistemas o recursos que no pertenezcan al área y que requieran conectarse con la red interna del área necesitan acuerdos certificados por parte de la administración de la seguridad de la información para proceder con dicha solicitud.

4.1.5 Seguridad Física y del Entorno

Se proponen las siguientes políticas para que las mismas sean gestionadas por el comité de seguridad asignado internamente y sean aplicadas únicamente en el área del NOC.

4.1.5.1 Políticas Diseñadas de Seguridad Física:

- Se propone implementar un sistema cerrado de vigilancia el cual utiliza 2 cámaras de seguridad monitoreadas las 24 horas, estas cámaras serán ubicadas en zonas estratégicas dentro del área que puedan abarcar toda la visión de la infraestructura física interna dentro del área.

- Se debe de tener sistemas contra incendios en el área y obligatoriamente un extintor dentro de la misma.

4.1.5.2 Políticas Diseñadas de Control de Acceso Físico:

- Se requieren mecanismos de control de acceso para el área, se pueden utilizar diversos sistemas de seguridad tales como los accesos biométricos en nuestro caso el registro de ingreso y salida de personal por medio de su huella digital y se tendrá el acceso únicamente de personal que labora en el área.

- Toda persona ajena al área que desee ingresar debe de registrarse informando el propósito de su visita y los datos personales e institucionales de dicha persona, de igual manera esto se aplica si la persona es encontrada dentro del área y en ambos casos se deberá informar al oficial de seguridad de la información.

- Todo personal que labora dentro del área tendrá que hacer uso de su credencial de trabajo de manera que sea fácilmente identificado por los administradores del área en nuestro caso el oficial de seguridad de la información.

- Se debe de limitar el acceso solo a personal autorizado a las zonas de acceso al cableado físico de energía, transmisión y recepción de datos, de igual manera se requiere proteger el cableado contra daños físicos e intercepciones.

- Se debe de registrar el ingreso y salida de todos los equipos físicos que estén o han estado en el área.

4.1.5.3 Políticas Diseñadas de Seguridad de Equipos Físicos:

- Los equipos no deben moverse o reubicarse sin previa autorización del responsable de activos.

- Tanto los equipos como los recursos van a ser utilizados y administrados únicamente por parte de personal interno del área.

- Todos los equipos deben someterse a mantenimientos periódicos según las especificaciones y recomendaciones de los proveedores.

- Respecto al retiro de equipos del área se requiere una previa autorización del responsable de activos y previo al retiro se debe de eliminar toda la información sensible que se contenga.

4.1.6 Gestión de Comunicaciones y Operaciones

Con la asignación de personal del área del NOC dentro del comité de seguridad de la información se asigna funciones y responsabilidades para la gestión del sistema de seguridad propuesto, cada funcionario del comité tiene su determinada función lo cual facilita la administración y reduce las

oportunidades de mal uso del sistema y el uso inadecuado de los activos dentro del área.

Se documentará la siguiente información respecto a los procesos gestionados dentro del área:

- Del monitoreo realizado de los enlaces se almacenan los datos de las gráficas generadas en el gestor CACTI.

- Respecto a la revisión lógica realizada se almacena la configuración, cambios y búsqueda realizada en el enrutamiento de los enlaces a nivel MPLS.

- Respecto a la revisión física se disponen de informes realizados por parte de personal de última milla después de culminar y atender las órdenes de revisión generadas en el sistema OPEN.

- Los mantenimientos preventivos manejan políticas similares a las órdenes generadas para revisión ya que se utilizan informes respecto al trabajo realizado por parte de personal de última milla encargado de realizar dicho mantenimiento.

- Toda esta información será almacenada en una base de datos administrada internamente en el área.

4.1.6.1 Políticas Diseñadas de Seguridad en Comunicaciones:

- Toda la información que concierne al uso de la red de datos utilizada internamente dentro del área como es la topología física de red, direccionamiento ip, medidas de seguridad, etc; debe clasificarse como información confidencial y reservada.

- Todas las conexiones a otras redes deben de contar con la gestión de la información en términos de autenticación, autorización, cifrado, detección de errores e intrusiones.

- La salida de información utilizada por el área hacia otras entidades debe de cumplir con acuerdos de confidencialidad.

- Se debe de verificar las características de los sistemas de información utilizados dentro del área de manera que al implementar nuevos sistemas no se provoque la interrupción de la funcionalidad de los aplicativos y utilitarios que utilizan los usuarios del área.

- Se prohibe el uso de software no autorizado por parte de personal del área.

- Se debe de utilizar herramientas de gestión de seguridad que respalden el uso o intercambio de información para garantizar la disponibilidad, confidencialidad e integridad de la misma, entre estas herramientas se gestionaría el uso de firewalls y antivirus.

- Se gestionará el registro de auditorías en donde se analice la identificación de usuarios, registro de fecha y hora de ingreso a los sistemas, intentos de ingreso y rechazos a los sistemas, cambios de configuración y uso de aplicaciones y herramientas.

4.1.6.2 Políticas Diseñadas para Almacenamiento y Respaldo:

- Toda la información utilizada y generada dentro del área debe de ser respaldada garantizando su disponibilidad, esta documentación será realizada en una base de datos manejada internamente en el área.

- Cada usuario del área es responsable de la información utilizada y almacenada en sus equipos de trabajo.

- Todo cambio realizado dentro del área será registrado e identificado ya que provocaría cambios en las políticas de seguridad propuestas.

4.1.7 Control de Acceso

Las políticas de seguridad de control de acceso para el área del NOC son gestionadas por el área de sistemas SIS, en éstas políticas se administran principalmente el uso de usuarios y contraseñas de cada usuario para el ingreso a las herramientas utilizadas dentro del área, de igual manera se gestionan los privilegios otorgados a cada usuario dependiendo de la función que desempeña dentro del área.

4.1.7.1 Políticas Diseñadas para el Uso de Contraseñas:

- Las contraseñas deben de contener caracteres alfanuméricos y como mínimo deben de estar conformadas de 8 caracteres.

- La contraseña debe de contener por lo menos una letra mayúscula y un número.

- Las contraseñas de los usuarios deben de cambiarse cada 120 días.

- Las contraseñas de los administradores deben de cambiarse cada 90 días.

- No debe de reutilizarse contraseñas antiguas.

4.1.7.2 Políticas Diseñadas para el Control de Acceso:

- Cada usuario debe disponer de un nombre de usuario y contraseña única.

- Las contraseñas son responsabilidad de sus propietarios. Dichas contraseñas serán generadas por el área de SIS y entregadas al usuario directamente.

- Las contraseñas solo deben ser conocidas por su propietario.

- Los usuarios son responsables de las actividades llevadas a cabo con su nombre de usuario y/o contraseña.

- Las contraseñas deben tener una fecha de caducidad definida en base a la sensibilidad de la información a proteger. Para los sistemas de acceso a las estaciones de trabajo, se recomienda cambiarlas cada 90 días. Las claves de administración deben cambiarse cada 60 días.

- Los nombres de usuario no deben estar basados en las funciones de trabajo. Los nombres de usuario identifican a personas específicas. Para la asignación de nombres de usuario se toma en cuenta la primera letra del nombre y el apellido completo del usuario, por ejemplo:
Sergio Ramos: sramos
Norman Páez: npaez

- En el caso de repetir la letra del nombre con otro usuario se añade la letra del segundo nombre a continuación, por ejemplo:
Luis Fernando Molina: lfmolina

- Se deben definir los perfiles de usuario de acuerdo a la función y cargo de los usuarios.

- El nivel de administrador de los sistemas críticos debe estar controlado. Es decir, las actividades realizadas por alguien con nivel/privilegio de administrador, deben ser supervisadas.

- Todos los equipos se bloquearán después de 10 min de inactividad y únicamente se ingresará nuevamente al sistema con el usuario y clave del personal que estaba utilizando el equipo.

- Respecto a cambios en el enrutamiento de red se requiere la autorización del responsable del área de tecnologías y se realizará la el registro y auditoría de dichos cambios.

- Se controlará el acceso a las aplicaciones y herramientas utilizadas dentro del área.

4.1.8 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

Las políticas de seguridad gestionadas por el área de sistemas SIS y que son aplicadas al área del NOC buscan como objetivo principal impartir normativas que garanticen la correcta utilización de la información de las aplicaciones, herramientas y gestores utilizados dentro del área.

4.1.8.1 Políticas Diseñadas para la Seguridad de la Información:

- Los usuarios del NOC son responsables de la información que manejan.

- Ningún personal del NOC debe suministrar cualquier información de la institución a ningún ente externo sin la autorización respectiva.

- Todos los usuarios tienen la responsabilidad de velar por la integridad, confidencialidad y disponibilidad de la información que maneje, especialmente si dicha información ha sido clasificada con algún nivel distinto al normal.

- Todo el personal debe firmar y renovar cada año, un acuerdo de confidencialidad y buen manejo de la información.

- Después de que el trabajador deje de prestar sus servicios en la empresa se compromete a entregar toda la información relacionada al trabajo realizado por él.

- Después de que el trabajador deje de prestar sus servicios, debe comprometerse a no utilizar, comercializar o divulgar la información generada o conocida durante su trabajo en la institución, directamente o través de terceros.

- La persona que detecte el mal uso de la información está en la obligación de reportar el hecho.

- Se requiere analizar los medios y comunicaciones utilizadas para la transferencia de información especialmente los de salida de información.

4.1.9 Gestión de los Incidentes de la Seguridad de la Información

La gestión de incidencias actualmente aplicada en el área del NOC no tendrá cambios en sus políticas y procedimientos utilizados, se utilizará las mismas políticas para la apertura, seguimiento, resolución y cierre de las incidencias actuales, dichas políticas son de uso interno y exclusivo del área.

Se tiene como prioridad la atención y solución inmediata de los problemas reportados por todos los clientes corporativos y gubernamentales a nivel nacional manteniendo y conservando la integridad, confidencialidad y disponibilidad de la información manejada internamente.

Los registros de incidentes gestionados se utilizarán para analizar e identificar las incidencias más recurrentes y que puedan afectar en la operación del área y de los enlaces que la misma maneja.

4.1.10 Gestión de la Continuidad del Negocio

Se detallarán las políticas propuestas para aplicarse al área del NOC para que la función del NOC no sea interrumpida por ningún evento fortuito o fallo en el sistema:

- Se dispondrá de equipamiento de respaldo ubicado en otra sucursal de la empresa en caso de siniestro o desastre natural que afecte las instalaciones y equipamiento utilizado en el edificio Doral en el área del NOC.

- La información será respaldada en la base de datos utilizada en el NOC así como en la base de datos administrada por el departamento de sistemas SIS de la empresa.

- Se realizará pruebas del plan de contingencia elaborado por el responsable del área de tecnologías, ésta prueba será en un entorno controlado y con el servicio interrumpido completamente en horarios en que la función del área no se vea afectada.

4.1.11 Cumplimiento

Algunas de las políticas de seguridad aplicadas por la gerencia nacional jurídica de la empresa CNT y que se aplican a todas las sucursales, áreas y personal a nivel nacional se detallarán a continuación:

4.1.11.1 Políticas Diseñadas de uso de Registros:

Se definen los documentos de registro que se requieran para el control de la actividad, de acuerdo a los lineamientos del sistema de seguridad diseñado, pudiéndose considerarse entre otros los siguientes:

- Registro de inspecciones.
- Registro y control de los soportes.
- Registro de software de nueva adquisición.
- Registro de entrada, salida y movimiento de tecnologías de información.
- Registro de incidencias de la Seguridad Informática.

4.1.11.2 Políticas Diseñadas sobre Software utilizado:

- El software utilizado debe garantizar la integridad de los datos.

- Se debe crear una cultura en los usuarios de la institución sobre las implicaciones del uso de software ilegal. Dicha cultura se fomentará mediante la publicación de boletines y/o charlas al respecto.

- Se mantendrá un inventario de las licencias de software de la empresa que permita su administración y control. El uso de este inventario permitirá detectar el uso de software no licenciado.

- Se establecerá un reglamento que limite el uso de software de demostración en las estaciones de la institución.

4.1.11.3 Políticas Diseñadas sobre actualización de Hardware:

- Cualquier alteración en la configuración del hardware (procesador, memoria, tarjetas adicionales, etc.) debe ser autorizado por el personal responsable de los recursos.

- La reparación de los equipos que implique la apertura de los mismos será realizada solo por personal autorizado.

- El movimiento y/o re-ubicación de equipos (PC, servidores, equipamiento activo) debe documentarse y estar debidamente autorizado.

4.1.11.4 Políticas Diseñadas sobre acceso a Redes de Alcance Global:

- Se dispondrá de un listado de usuarios autorizados, especificando nombre, apellidos y cargo que ocupa en la institución, así como los servicios para los que está autorizado.

4.2 Factores Considerados para la Implementación del SGSI

Para poder analizar una posible implementación del SGSI propuesto se deben de considerar ciertos factores para que dicha implementación pueda alcanzarse con éxito y se alcancen los objetivos propuestos en el SGSI conforme las exigencias del área lo requieran.

4.2.1 Compromiso de los Altos Directivos del Área del NOC

Para poder implementar el SGSI propuesto se requiere el respaldo y compromiso formal de la gerencia y directivos del área, con esto el oficial de seguridad asignado en el comité dentro del área conseguirá las atribuciones y autoridad necesaria para poder implementar las políticas propuestas.

4.2.2 Fondo Financiero para la Implementación del SGSI

Se requiere contar con un fondo financiero que permita adquirir los recursos necesarios que el oficial de seguridad de la información proponga utilizar para poder implementar el SGSI propuesto.

4.3 Análisis de Restricciones para Implementar el SGSI

Existen algunas restricciones que pueden ocasionar un fallo en la implementación del SGSI propuesto entre ellas tenemos las siguientes:

4.3.1 Restricciones de Tiempo

Por la evaluación del sistema propuesto, pruebas realizadas de funcionamiento y su puesta en función dentro del área la implementación del sistema puede demorar un tiempo considerable.

El tiempo dedicado por parte del personal dentro del área también es otra restricción ya que aparte del tiempo aplicado en las funciones desempeñadas habitualmente dentro del área el personal asignado que conforma el comité de seguridad deberá aplicar tiempo en la evaluación, implementación y capacitación de las políticas propuestas en el SGSI.

4.3.2 Restricciones Financieras

El presupuesto para la implementación del SGSI no puede ser suficiente para abarcar todos los requerimientos que contemplan las políticas de seguridad propuestas.

4.3.3 Restricciones de Recurso Humano

La carencia de personal capacitado en seguridad de la información puede ser una restricción para poder implementar el SGSI propuesto e incluso puede afectar en el buen funcionamiento del mismo.

4.4 Análisis de Posibles Soluciones para Poder Implementar el SGSI

4.4.1 Soluciones de Tiempo

Se debe de crear un cronograma de implementación en el cual se establezcan tiempos de cumplimiento para cada objetivo del SGSI propuesto dentro del área, con esto se logra minimizar al máximo posibles atrasos en la implementación.

4.4.2 Soluciones de Financiamiento

Se requiere un análisis de factibilidad económica el cual permita conocer el presupuesto necesario para poder implementar el sistema y así evitar pérdidas de recursos.

4.4.3 Soluciones para Uso de Personal

Establecer cronogramas para impartir capacitaciones fuera del horario laboral, estas capacitaciones pueden incluir aulas virtuales a las cuales personal del área pueda acceder en cualquier horario y de cualquier lugar con conexión a internet.

4.5 Análisis de Factibilidad

4.5.1 Factibilidad Técnica

Se describirán las características de los equipos y del software necesario para poder implementar el SGSI propuesto.

Para la utilización del sistema Alfresco que es una herramienta para gestión de información y documentación se requiere un equipo con las siguientes características:

Características	Capacidad
Sistema Operativo	Windows Server 2003 o superior de 32 o 64 bits
Disco Duro	500 GB
Memoria RAM	1 GB
Procesador	Dual Core 2.5 GHz
Tarjeta de Red	100 Mbps
Fuente de Alimentación Ininterrumpida	350VA 120V

Figura 26. Características del Servidor para Alfresco

Tomado de Pontificia Universidad Católica del Perú, s.f.

Para la gestión de control de acceso físico se requiere el siguiente equipamiento:

- Cámaras de Vigilancia.
- Lector de Huella Digital.

El área al momento dispone de todos los equipos mencionados con las características requeridas por lo que no se procederá con la adquisición de los mismos.

No se requiere realizar cambios ni adiciones de equipos en la infraestructura actualmente utilizada por lo que se concluye que se puede proceder con la implementación del SGSI propuesto.

4.5.2 Factibilidad Económica

Se obtiene un estimado de los costos económicos necesarios para poder implementar el SGSI propuesto (Tabla 12).

Se requiere la valoración de los siguientes recursos:

Tabla 12. Presupuesto

RECURSO	VALOR ESTIMADO
Servidor para la gestión de la herramienta Alfresco	3000$
Firewall	1500$
Cámaras de Seguridad	3000$
Lector de Huellas Digitales	300$
Antivirus	1000$
Capacitación	1000$
Implementación de Aulas Virtuales	500$
Protección de Cableado	500$
Personal Encargado de la Implementación	16000$
TOTAL:	**26800$**

El valor total estimado es 26800$ en el caso que se requiera implementar el SGSI considerando que no se dispongan de los recursos mencionados.

Actualmente la empresa específicamente el área del NOC dispone de la mayoría de recursos requeridos para la implementación del SGSI, en el caso de proceder con la implementación del SGSI propuesto únicamente se va a necesitar invertir en la capacitación e implementación de las aulas virtuales concluyendo que el valor estimado de implementación del SGSI sería 1500$.

4.6 Guía de Implementación

Para poder concretar la implementación del SGSI se recomienda seguir los siguientes pasos en el orden indicado:

- Análisis del marco legal.
- Análisis del estado actual de la seguridad de la información en el área del NOC.
- Aprobación del SGSI propuesto y el presupuesto necesario.
- Puesta en función de Alfresco.
- Identificación de activos.
- Análisis de vulnerabilidades.
- Evaluación y tratamiento de riesgos.
- Elaboración de políticas.
- Implementación de aulas virtuales.
- Capacitación a los funcionarios.
- Implementación de las políticas.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

El sistema de gestión de seguridad de la información SGSI propuesto tiene como objetivo aplicar políticas de seguridad que sean utilizadas únicamente dentro del área del NOC siendo un área crítica por la función e información manejada internamente.

La información manejada internamente en el área del NOC es catalogada como confidencial y de uso exclusivo del área por lo que las políticas propuesta en el SGSI busca como objetivo garantizar el buen manejo y una correcta gestión de la información por parte de los usuarios dentro del área.

La infraestructura física y tecnológica actualmente utilizada en el área del NOC se puede utilizar sin realizar cambios ni adiciones en dicha infraestructura para poder implementar el SGSI propuesto.

Algunas políticas del SGSI actualmente utilizado en la empresa el mismo que es gestionado por el área de SIS son aplicadas directamente al área del NOC sin proponer cambios en el actual proyecto.

Es necesario capacitar a todo el personal del área del NOC respecto a políticas y normas de seguridad de la información antes y después de la implementación del SGSI propuesto.

El comité de seguridad de la información seleccionado es el único grupo de personas dentro del área que puede administrar el SGSI propuesto.

RECOMENDACIONES

Todo tipo de SGSI que se pretenda implementar se recomienda realizarlo en el menor tiempo posible antes de que se produzcan cambios en la gestión y funcionalidad del área en donde se planifique implementar el SGSI.

Las capacitaciones impartidas al personal que labora dentro del área donde se va a implementar el SGSI se deben de realizar periódicamente en horarios que no afecten la gestión del área.

El compromiso de los directivos es indispensable para poner en marcha cualquier sistema de gestión de seguridad de la información.

Debido a que el SGSI propuesto es diseñado para aplicarse únicamente al área del NOC se requiere seleccionar directivos dentro del área para que conformen el comité de seguridad el cual se encargará de la administración de las políticas.

Para proceder con la implementación del SGSI propuesto se requiere el análisis y aprobación del Gerente de área.

REFERENCIAS

Escuela Superior Politécnica de Chimborazo. (2010). *Tesis de Grado: Diseño de la Gestión de Seguridad y Salud Ocupacional en el Ingenio Azucarero San Carlos S.A.* Ecuador.

Fiscalía General del Estado. (s.f.). *Caso: Ministerio de Ambiente Los 11 procesados rindieron sus versiones.* Recuperado el 2 de marzo de 2015 http://goo.gl/qyuUHf

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (s.f.). *Sistema de Gestión de Seguridad de la Información (SGSI).* Recuperado el 2 de marzo de 2015 http://www.iso27000.es/sgsi.html

Pontificia Universidad Católica del Perú (2009). *Tesis de Grado: Diseño de un Sistema Básico de Gestión de Seguridad de Información para Centros Educativos Parroquiales.* Ecuador.

Saucedo, G. y Jeimy, C. (2012). *IV Encuesta Latinoamericana de Seguridad de la Información.* Ecuador: Tendencias.

Secretaría Nacional de la Administración Pública. (2009). *Instituto Ecuatoriano de Normalización*. Ecuador: INEN-ISO.

Secretaría Nacional de la Administración Pública. (2013). *Esquema Gubernamental de Seguridad de la Información.* Ecuador: Registro Oficial.

Universidad de los Andes. (s.f.). . *Metodología de la Gestión de Riesgos de Tecnologías de la Información.* Recuperado el 2 de marzo de 2015 https://revistaing.uniandes.edu.co/

Universidad de los Andes. (s.f.). . *Metodología de la Gestión de Riesgos de Tecnologías de la Información.* Recuperado el 2 de marzo de 2015 http://vmwiso01.andinatel.int/27000/27000/sdi/index.php

Universidad de los Andes. (s.f.). . *Metodología de la Gestión de Riesgos de Tecnologías de la Información.* Recuperado el 2 de marzo de 2015 http://www.contraloria.gob.ec/documentos/normatividad/NTCI-PRES-INDICE.pdf

Universidad de los Andes. (s.f.). . *Metodología de la Gestión de Riesgos de Tecnologías de la Información.* Recuperado el 2 de marzo de 2015 http://documentacion.asambleanacional.gob.ec/alfresco/d/d/workspace/SpacesStore/ea7d10c2-791a-4e01-8ef6 f60e22ced64f/Ley%20de%20Protecci%C3%B3n%20a%20la%20Intimidad%20y%20a%20los%20Datos%20Personales

Universidad de los Andes. (s.f.). . *Metodología de la Gestión de Riesgos de Tecnologías de la Información.* Recuperado el 2 de marzo de 2015 http://registromercantil.gob.ec/loja/ley-de-transparencia-loja/Loja/2013/2.%20Informaci%C3%B3n%20Legal/Normas%20de%20Regulaci%C3%B3n/Ley%20del%20Sistema%20Nacional%20de%20Registro%20De%20Datos%20P%C3%BAblicos.pdf/detail.html

Universidad de los Andes. (s.f.). . *Metodología de la Gestión de Riesgos de Tecnologías de la Información.* Recuperado el 2 de marzo de 2015 http://www.cdc.gob.cl/wp-content/uploads/documentos/legislacion_internacional/ley_organica_de_acceso_a_la_informacion_en_ecuador.pdf

Universidad de los Andes. (s.f.). . *Metodología de la Gestión de Riesgos de Tecnologías de la Información.* Recuperado el 2 de marzo de 2015 http://www.iso27000.es/download/doc_iso27000_all.pdf

Universidad de los Andes. (s.f.). . *Metodología de la Gestión de Riesgos de Tecnologías de la Información.* Recuperado el 2 de marzo de 2015 http://www.iso.org/iso/home.html

Universidad de los Andes. (s.f.). . *Metodología de la Gestión de Riesgos de Tecnologías de la Información.* Recuperado el 2 de marzo de 2015 http://www.acis.org.co/revistasistemas/images/stories/Edicion123/ed123jeimyivinforme_elsi2012.pdf

Universidad de los Andes. (s.f.). . *Metodología de la Gestión de Riesgos de Tecnologías de la Información.* Recuperado el 2 de marzo de 2015 http://www.contraloria.gob.ec/documentos/normatividad/Acuerdo026-CG-2015ManualsustitutivoBalcondeServicios.pdf

Universidad de los Andes. (s.f.). . *Metodología de la Gestión de Riesgos de Tecnologías de la Información.* Recuperado el 2 de marzo de 2015 http://www.tp-link.com/co/products/details/cat-4792_MC112CS.html#specifications

Universidad de los Andes. (s.f.). . *Metodología de la Gestión de Riesgos de Tecnologías de la Información.* Recuperado el 2 de marzo de 2015 http://www.abox.com/productos.asp?pid=277

Universidad de los Andes. (s.f.). . *Metodología de la Gestión de Riesgos de Tecnologías de la Información.* Recuperado el 2 de marzo de 2015 http://www.tp-link.com/ar/products/details/cat-42_TL-SF1016D.html#features

Universidad de los Andes. (s.f.). . *Metodología de la Gestión de Riesgos de Tecnologías de la Información.* Recuperado el 2 de marzo de 2015 http://www.dlink.com/-/media/Business_Products/DGS/DGS%201016D/Datasheet/DGS_1016D_Datasheet_v1_Sept_2009_EN_UK.pdf

Universidad de los Andes. (s.f.). . *Metodología de la Gestión de Riesgos de Tecnologías de la Información.* Recuperado el 2 de marzo de 2015 http://www.dlink.com/-/media/Business_Products/DGS/DGS%201016D/Datasheet/DGS_1016D_Datasheet_v1_Sept_2009_EN_UK.pdf

Universidad de los Andes. (s.f.). . *Metodología de la Gestión de Riesgos de Tecnologías de la Información.* Recuperado el 2 de marzo de 2015 http://corporativo.cnt.gob.ec/estructura-organica/#!prettyPhoto

ANEXOS

ANEXO 1 ESTÁNDAR INTERNACIONAL ISO-IEC 27001

ESTÁNDAR INTERNACIONAL **ISO/IEC 27001**

Primera Edicion
2005 - 10 - 15

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

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

Tabla de Contenido

Prefacio

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

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

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

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

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

0 Introducción

0.1 General

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

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

0.2 Enfoque del Proceso

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

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

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

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

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

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

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

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

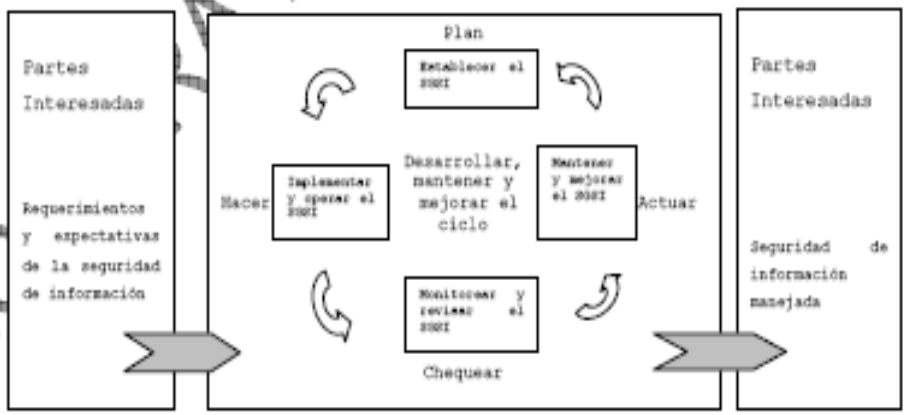
EJEMPLO 1

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

EJEMPLO 2

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

Figura 1 – Modelo PDCA aplicado a los procesos SGSI



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

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

0.3 Compatibilidad con otros sistemas de gestión

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

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

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

1 Alcance

1.1 General

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

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

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

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

1.2 Aplicación

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

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

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

2 Referencias normativas

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

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

3 Términos y definiciones

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

3.1
activo

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

3.2
disponibilidad

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

3.3

confidencialidad

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

(ISO/IEC 13335-1:2004)

3.4

seguridad de información

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

(ISO/IEC 17799:2005)

3.5

evento de seguridad de la información

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

(ISO/IEC TR 18044:2004)

3.6

incidente de seguridad de la información

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

(ISO/IEC TR 18044:2004)

3.7

sistema de gestión de seguridad de la información SGSI

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

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

3.8

integridad

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

(ISO/IEC 13335-1:2004)

3.9

riesgo residual

el riesgo remanente después del tratamiento del riesgo

(ISO/IEC Guía 73:2002)

3.10

aceptación de riesgo

decisión de aceptar el riesgo

(ISO/IEC Guía 73:2002)

3.11

análisis de riesgo

uso sistemático de la información para identificar fuentes y para estimar el riesgo

(ISO/IEC Guía 73:2002)

3.12

valuación del riesgo

proceso general de análisis del riesgo y evaluación del riesgo

(ISO/IEC Guía 73:2002)

3.13

evaluación del riesgo

proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo

(ISO/IEC Guía 73:2002)

3.14

gestión del riesgo

actividades coordinadas para dirigir y controlar una organización con relación al riesgo

(ISO/IEC Guía 73:2002)

3.15

tratamiento del riesgo

proceso de tratamiento de la selección e implementación de medidas para modificar el riesgo

(ISO/IEC Guía 73:2002)

NOTA: En este Estándar Internacional el término 'control' se utiliza como sinónimo de 'medida'.

3.16

enunciado de aplicabilidad

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

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

4 Sistema de gestión de seguridad de la información

4.1 Requerimientos generales

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

4.2 Establecer y manejar el SGSI

4.2.1 Establecer el SGSI

La organización debe hacer lo siguiente:

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

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

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

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

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

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

5) haya sido aprobada por la gerencia.

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

c) Definir el enfoque de valuación del riesgo de la organización
   1) Identificar una metodología de cálculo del riesgo adecuado para el SGSI y los requerimientos identificados de seguridad, legales y reguladores de la información comercial.
   2) Desarrollar los criterios para aceptar los riesgos e identificar los niveles de riesgo aceptables (ver 5.1f).

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

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

d) Identificar los riesgos
   1) Identificar los activos dentro del alcance del SGSI y los propietarios[2] de estos activos.
   2) Identificar las amenazas para aquellos activos.
   3) Identificar las vulnerabilidades que podrían ser explotadas por las amenazas.
   4) Identificar los impactos que pueden tener las pérdidas de confiabilidad, integridad y disponibilidad sobre los activos.

e) Analizar y evaluar el riesgo
   1) Calcular el impacto comercial sobre la organización que podría resultar de una falla en la seguridad, tomando en cuenta las consecuencias de una pérdida de confidencialidad, integridad o disponibilidad de los activos.
   2) Calcular la probabilidad realista de que ocurra dicha falla a la luz de las amenazas y vulnerabilidades prevalecientes, y los impactos asociados con estos activos, y los controles implementados actualmente.
   3) Calcular los niveles de riesgo.

---

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

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

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

Las acciones posibles incluyen:

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

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

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

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

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

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

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

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

j) Preparar un Enunciado de Aplicabilidad

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

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

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

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

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

4.2.2 Implementar y operar el SGSI

La organización debe hacer lo siguiente:

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

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

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

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

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

f) Manejar las operaciones del SGSI.

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

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

4.2.3 Monitorear y revisar el SGSI

La organización debe hacer lo siguiente:

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

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

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

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

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

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

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

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

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

4.2.4 Mantener y mejorar el SGSI

La organización debe realizar regularmente lo siguiente:

a) Implementar las mejoras identificadas en el SGSI.

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

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

d) Asegurar que las mejoras logren sus objetivos señalados.

4.3 Requerimientos de documentación

4.3.1 General

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

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

La documentación SGSI debe incluir lo siguiente:

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

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

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

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

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

4.3.2 Control de documentos

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

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

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

4.3.3 Control de registros

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

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

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

5 Responsabilidad de la gerencia

5.1 Compromiso de la gerencia

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

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

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

5.2 Gestión de recursos

5.2.1 Provisión de recursos

La organización debe determinar y proporcionar los recursos necesarios para:

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

5.2.2 Capacitación, conocimiento y capacidad

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

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

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

6 Auditorías internas SGSI

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

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

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

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

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

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

7 Revisión Gerencial del SGSI

7.1 General

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

7.2 Insumo de la revisión

El insumo para la revisión gerencial debe incluir:

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

7.3 Resultado de la revisión

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

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

8 Mejoramiento del SGSI

8.1 Mejoramiento continuo

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

8.2 Acción correctiva

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

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

8.3 Acción preventiva

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

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

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

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

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

Anexo A

(Normativo)

Objetivos de control y controles

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

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

Tabla A.1 – Objetivos de control y controles

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Anexo B

(Informativo)

Principios OECD y este Estándar Internacional

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

Tabla B.1 – Principios OECD y el modelo PDCA

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

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

Anexo C

(Informativo)

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

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

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

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

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

Bibliografía

Publicación de estándares

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

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

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

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

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

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

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

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

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

Otras publicaciones

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

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

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

ANEXO 2 CERTIFICACIÓN ISO 27001 ACTA REUNIÓN

Levantamiento de Procesos y Activos de Información Relacionados al SGSI

Quito, 18 de septiembre del 2013
Lugar: Despacho Gerencia General CNT EP

Participantes en la Reunión

Nombre	Empresa	Firma
César Regalado Gerente General	CNT EP	
Ana Yépez Delegada Gerencia General al SGSI	CNT EP	
Ximena Carrión Gerente de Clientes Corporativos RG2	CNT EP	
Rocío Espinosa Gerente Nacional de TI	CNT EP	
Yandry Castro Oficial de Seguridad de la Información	CNT EP	
José Pino Encargado del SGSI	CNT EP	

Temas Tratados

- Estatus de acciones correctivas del SGSI de la fase 1 de la auditoría de certificación
- Estatus proceso de actualización del SGSI
  - Revisión del Manual del SGSI
  - Revisión de la Política de Seguridad de la Información
  - Actualización del inventario de activos de información
  - Evaluación de riesgos
  - Actualización de procedimientos
- Revisión de los resultados de la Auditoría Interna al SGSI
- Revisión del plan de acción de medidas correctivas
- Preparación para el inicio de fase 2 de la auditoría de certificación
- Recomendaciones para el mejoramiento

Resultado de la revisión

- Ejecución del plan de acción como medida correctiva de la auditoría interna del SGSI

ANEXO 3 REGISTRO OFICIAL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

REGISTRO OFICIAL

ÓRGANO DEL GOBIERNO DEL ECUADOR

Administración del Sr. Ec. Rafael Correa Delgado
Presidente Constitucional de la República

SEGUNDO SUPLEMENTO

Año I - Nº 88

Quito, miércoles 25 de septiembre de 2013

Valor: US$ 1.25 + IVA

ING. HUGO ENRIQUE DEL POZO BARREZUETA
DIRECTOR

Quito: Avenida 12 de Octubre N 16-90 y Pasaje Nicolás Jiménez

Dirección: Telf. 2901 - 629
Oficinas centrales y ventas:
Telf. 2234 - 540

Distribución (Almacén):
Mañosca Nº 201 y Av. 10 de Agosto
Telf. 2430 - 110

Sucursal Guayaquil:
Malecón Nº 1606 y Av. 10 de Agosto
Telf. 2527 - 107

Suscripción anual: US$ 400 + IVA para la ciudad de Quito
US$ 450 + IVA para el resto del país
Impreso en Editora Nacional

40 páginas

www.registroficial.gob.ec

Al servicio del país
desde el 1º de julio de 1895

Secretaría Nacional de la Administración Pública

No. 166

Cristian Castillo Peñaherrera
SECRETARIO NACIONAL DE LA ADMINISTRACIÓN PÚBLICA

Considerando:

Que, la Constitución de la República determina en el artículo 227 que la Administración Pública constituye un servicio a la colectividad que se rige por principios de eficacia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación.

Que, el artículo 13 del Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva establece que la Secretaría Nacional de la Administración Pública es una entidad de derecho público, con personalidad jurídica y patrimonio propio, dotada de autonomía presupuestaria, financiera, económica y administrativa, encargada de establecer las políticas, metodologías de gestión e innovación institucional y herramientas necesarias para el mejoramiento de la eficiencia, calidad y transparencia de la gestión en las entidades y organismos de la Función Ejecutiva, con quienes coordinará las

acciones que sean necesarias para la correcta ejecución de dichos fines; así como también de realizar el control, seguimiento y evaluación de la gestión de los planes, programas, proyectos y procesos de las entidades y organismos de la Función Ejecutiva que se encuentren en ejecución; y, el control, seguimiento y evaluación de la calidad en la gestión de los mismos.

Que, mediante Acuerdos Ministeriales Nos. 804 y 837 de 29 de julio y 19 de agosto de 2011, respectivamente, la Secretaría Nacional de la Administración Pública creó la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación conformada por delegados del Ministerio de Telecomunicaciones y de la Sociedad de la Información, la Secretaría Nacional de Inteligencia y la Secretaría Nacional de la Administración Pública y dentro de sus atribuciones tiene la de establecer lineamientos de seguridad informática, protección de infraestructura computacional y todo lo relacionado con ésta, incluyendo la información contenida para las entidades de la Administración Pública Central e Institucional.

Que, es importante adoptar políticas, estrategias, normas, procesos, procedimientos, tecnologías y medios necesarios para mantener la seguridad en la información que se genera y custodia en diferentes medios y formatos de las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva.

Que, la Administración Pública de forma integral y coordinada debe propender a minimizar o anular riesgos en la información así como proteger la infraestructura gubernamental, más aún si es estratégica, de los denominados ataques informáticos o cibernéticos.

Que, las Tecnologías de la Información y Comunicación son herramientas imprescindibles para el cumplimiento de la gestión institucional e inter-institucional de la Administración Pública en tal virtud, deben cumplir con estándares de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información;

Que, la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación en referencia ha desarrollado el Esquema Gubernamental de Seguridad de la Información (EGSI), elaborado en base a la norma NTE INEN-ISO/IEC 27002 "Código de Práctica para la Gestión de la Seguridad de la Información".

Que, el artículo 15, letra i) del Estatuto del Régimen Jurídico y Administrativo de la Función Ejecutiva establece como atribución del Secretario Nacional de la Administración Pública, impulsar proyectos de estandarización en procesos, calidad y tecnologías de la información y comunicación,

En uso de las facultades y atribuciones que le confiere el artículo 15, letra n) del Estatuto del Régimen Jurídico y Administrativo de la Función Ejecutiva,

Acuerda:

Artículo 1.- Disponer a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información.

Artículo 2.- Las entidades de la Administración Pública implementarán en un plazo de dieciocho (18) meses el Esquema Gubernamental de Seguridad de la Información (EGSI), que se adjunta a este acuerdo como Anexo 1, a excepción de las disposiciones o normas marcadas como prioritarias en dicho esquema, las cuales se implementarán en (6) meses desde la emisión del presente Acuerdo.

La implementación del EGSI se realizará en cada institución de acuerdo al ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de Seguridad de la Información.

Artículo 3.- Las entidades designarán, al interior de su institución, un Comité de Seguridad de la Información liderado con un Oficial de Seguridad de la Información, conforme lo establece el EGSI y cuya designación deberá ser comunicada a la Secretaría Nacional de la Administración Pública, en el transcurso de treinta (30) días posteriores a la emisión del presente Acuerdo.

Artículo 4.- La Secretaría Nacional de la Administración Pública coordinará y dará seguimiento a la implementación del EGSI en las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva. El seguimiento y control a la implementación de la EGSI se realizará mediante el Sistema de Gestión por Resultados (GPR) u otras herramientas que para el efecto implemente la Secretaría Nacional de la Administración Pública.

Artículo 5.- La Secretaría Nacional de la Administración Pública realizará de forma ordinaria una revisión anual del EGSI en conformidad a las modificaciones de la norma INEN ISO/IEC 27002 que se generen y de forma extraordinaria o periódica cuando las circunstancias así lo ameriten, además definirá los procedimientos o metodologías para su actualización, implementación, seguimiento y control.

Artículo 6.- Es responsabilidad de la máxima autoridad de cada entidad mantener la documentación de la implementación del EGSI debidamente organizada y registrada de acuerdo al procedimiento específico que para estos efectos establezca la Secretaría Nacional de la Administración Pública.

Artículo 7.- Las entidades realizarán una evaluación de riesgos y diseñarán e implementarán el plan de manejo de riesgos de su institución, en base a la norma INEN ISO/IEC 27005 "Gestión del Riesgo en la Seguridad de la Información".

DISPOSICIONES GENERALES

Primera.- El EGSI podrá ser revisado periódicamente de acuerdo a las sugerencias u observaciones realizadas por las entidades de la Administración Pública Central, Institucional o que dependen de la Función Ejecutiva, las cuales deberán ser presentadas por escrito a la Secretaría Nacional de la Administración Pública.

Segunda.- Cualquier propuesta de inclusión de controles o directrices adicionales a los ya establecidos en el EGSI que se generen en la implementación del mismo, deberán ser comunicados a la Secretaría Nacional de la Administración Pública, previo a su aplicación; de igual manera, en caso de existir alguna excepción institucional respecto a la implementación del EGSI, ésta deberá ser justificada técnicamente y comunicada a la Secretaría Nacional de la Administración Pública, para su análisis y autorización.

Tercera.- Los Oficiales de Seguridad de la Información de los Comités de Gestión de Seguridad de la Información designados por las instituciones, actuarán como contrapartes de la Secretaría Nacional de la Administración Pública en la implementación del EGSI y en la gestión de incidentes de seguridad de la información.

Cuarta.- Cualquier comunicación respecto a las disposiciones realizadas en el presente Acuerdo deberá ser informada directamente a la Subsecretaría de Gobierno Electrónico de la Secretaría Nacional de la Administración Pública.

DISPOSICIONES TRANSITORIAS

Primera.- Para efectivizar el control y seguimiento del EGSI institucional, la Secretaría Nacional de la Administración Pública en un plazo de quince (15) días creará un proyecto en el sistema GPR en el que se homogenice los hitos que deben de cumplir las instituciones para implementar el EGSI.

Segunda.- La Secretaría Nacional de la Administración Pública emitirá en el plazo de sesenta (60) días desde la emisión del presente Acuerdo los lineamientos específicos de registro y documentación de la implementación institucional del EGSI.

Tercera.- La Secretaría Nacional de la Administración Pública, además, en un plazo de noventa (90) días desde la emisión del presente Acuerdo, definirá las metodologías o procedimientos para actualización, implementación, seguimiento y control del EGSI.

DISPOSICIÓN DEROGATORIA

Derógase los Acuerdo Ministeriales No. 804 de 29 de julio de 2011 y No. 837 de 19 de agosto de 2011.

DISPOSICION FINAL.- Este Acuerdo entrará en vigencia a partir de su publicación en el Registro Oficial.

Dado en el Palacio Nacional, a los 19 días del mes de septiembre de 2013.

f.) Cristian Castillo Peñaherrera, Secretario Nacional de la Administración Pública.

Es fiel copia del original - LO CERTIFICO.

Quito, 20 de septiembre de 2013.

f.) Dra. Rafaela Hurtado Espinoza, Coordinadora General de Asesoría Jurídica, Secretaría Nacional de la Administración Pública.

Anexo 1 del Acuerdo No. 166 del 19 de septiembre de 2013

SECRETARÍA NACIONAL DE LA ADMINISTRACIÓN PÚBLICA

ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI)

Versión 1.0

Septiembre de 2013

Contenido

INTRODUCCIÓN

Los avances de las Tecnologías de la Información y Comunicación (TIC) han ocasionado que los gobiernos otorguen mayor atención a la protección de sus activos de información con el fin de generar confianza en la ciudadanía, en sus propias instituciones y minimizar riesgos derivados de vulnerabilidades informáticas.

La Secretaría Nacional de Administración Pública, considerando que las TIC son herramientas imprescindibles para el desempeño de institucional e inter-institucional, y como respuesta a la necesidad gestionar de forma eficiente y eficaz la seguridad de la información en las entidades públicas, emitió los Acuerdos Ministeriales No. 804 y No. 837, de 29 de julio y 19 de agosto de 2011 respectivamente, mediante los cuales creó la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación.

La comisión realizó un análisis de la situación respecto de la gestión de la Seguridad de la Información en las Instituciones de la Administración Pública Central, Dependiente e Institucional, llegando a determinar la necesidad de aplicar normas y procedimientos para seguridad de la información, e incorporar a la cultura y procesos institucionales la gestión permanente de la misma.

El presente documento, denominado Esquema Gubernamental de Seguridad de la Información (EGSI), esta basado en la norma técnica ecuatoriana INEN ISO/IEC 27002 para Gestión de la Seguridad de la Información y está dirigido a las Instituciones de la Administración Pública Central, Dependiente e Institucional.

El EGSI establece un conjunto de directrices prioritarias para Gestión de la Seguridad de la Información e inicia un proceso de mejora continua en las instituciones de la Administración Pública. El EGSI no reemplaza a la norma INEN ISO/IEC 27002 sino que marca como prioridad la implementación de algunas directrices.

La implementación del EGSI incrementará la seguridad de la información en las entidades públicas así como en la confianza de los ciudadanos en la Administración Pública.

1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1.1. Documento de la Política de la Seguridad de la Información

a) La máxima autoridad de la institución dispondrá la implementación de este Esquema Gubernamental de Seguridad de la Información (EGSI) en su entidad (*)[1].

b) Se difundirá la siguiente política de seguridad de la información como referencia (*):

"Las entidades de la Administración Pública Central, Dependiente e Institucional que generan, utilizan, procesan, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el Esquema Gubernamental de Seguridad de la Información para definir los procesos, procedimientos

[1] (*) En todo este documento esta marca significa que se trata de un control/directriz prioritario

y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad lo requiera".

Las entidades públicas podrán especificar una política de seguridad más amplia o específica en armonía con la Constitución, leyes y demás normativa legal propia o relacionada así como su misión y competencias.

1.2. Revisión de la Política

a) Para garantizar la vigencia de la política de seguridad de la información en la institución, esta deberá ser revisada anualmente o cuando se produzcan cambios significativos a nivel operativo, legal, tecnológico, económico, entre otros.

2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

2.1. Compromiso de la máxima autoridad de la institución con la seguridad de la información

a) Realizar el seguimiento de la puesta en marcha de las normas de este documento (*).

b) Disponer la difusión, capacitación y sensibilización del contenido de este documento (*).

c) Conformar oficialmente el Comité de Gestión de la Seguridad de la Información de la institución (CSI) y designar a los integrantes (*).

El comité de coordinación de la seguridad de la información involucrará la participación y cooperación de los cargos directivos de la institución. El comité deberá convocarse de forma periódica o cuando las circunstancias lo ameriten. Se deberá llevar registros y actas de las reuniones.

2.2. Coordinación de la Gestión de la Seguridad de la Información

a) La coordinación estará a cargo del Comité de Gestión de Seguridad de la Información el cual tendrá las siguientes funciones:

- Definir y mantener la política y normas institucionales particulares en materia de seguridad de la información y gestionar la aprobación y puesta en vigencia por parte de la máxima autoridad de la institución así como el cumplimiento por parte de los funcionarios de la institución.
- Monitorear cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.
- Acordar y aprobar metodologías y procesos específicos, en base al EGSI relativos a la seguridad de la información.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios, en base al EGSI.
- Promover la difusión y apoyo a la seguridad de la información dentro de la institución.
- Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la institución frente a incidentes de seguridad imprevistos.
- Designar a los custodios o responsables de la información de las diferentes áreas de la entidad, que deberá ser formalizada en un documento físico o electrónico.
- Gestionar la provisión permanente de recursos económicos, tecnológicos y humanos para la gestión de la seguridad de la información.
- Velar por la aplicación de la familia de normas técnicas ecuatorianas INEN ISO/IEC 27000 en la institución según el ámbito de cada norma.
- Designar formalmente a un funcionario como Oficial de Seguridad de la Información quien actuará como coordinador del CSI. El Oficial de Seguridad no pertenecerá al área de Tecnologías de la Información y reportará a la máxima autoridad de la institución (*).
- Designar formalmente al responsable de seguridad del área de Tecnologías de la Información en coordinación con el director o responsable del área de Tecnologías de la Información de la institución (*).

2.3 Asignación de responsabilidades para la seguridad de la información

El Oficial de Seguridad de la Información tendrá las siguientes responsabilidades:

a) Definir procedimientos para el control de cambios a los procesos operativos, los sistemas e instalaciones, y verificar su cumplimiento, de manera que no afecten la seguridad de la información.

b) Establecer criterios de seguridad para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas antes de su aprobación definitiva.

c) Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento.

d) Controlar los mecanismos de distribución y difusión de información dentro y fuera de la institución.

e) Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso, garantizar la seguridad de los datos y los servicios conectados a las redes de la institución.

f) Desarrollar procedimientos adecuados de concienciación de usuarios en materia de seguridad, controles de acceso a los sistemas y administración de cambios.

g) Verificar el cumplimiento de las normas, procedimientos y controles de seguridad institucionales establecidos.

h) Coordinar la gestión de eventos de seguridad con otras entidades gubernamentales.

i) Convocar regularmente o cuando la situación lo amerite al Comité de Seguridad de la Información así como llevar registros de asistencia y actas de las reuniones.

El responsable de Seguridad del Área de Tecnologías de la Información tendrá las siguientes responsabilidades:

a) Controlar la existencia de documentación física o electrónica actualizada relacionada con los procedimientos de comunicaciones, operaciones y sistemas.

b) Evaluar el posible impacto operativo a nivel de seguridad de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando responsabilidades.

c) Administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento.

d) Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad para soportar potenciales amenazas a la seguridad de la información que procesan.

e) Controlar la obtención de copias de resguardo de información, así como la prueba periódica de su restauración.

f) Asegurar el registro de las actividades realizadas por el personal operativo de seguridad de la información, para su posterior revisión.

g) Desarrollar y verificar el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.

h) Implementar los controles de seguridad definidos (ej., evitar software malicioso, accesos no autorizados, etc.).

i) Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento (ej., cintas, discos, etc.) e informes impresos, y verificar la eliminación o destrucción segura de los mismos, cuando proceda.

j) Gestionar los incidentes de seguridad de la información de acuerdo a los procedimientos establecidos.

k) Otras que por naturaleza de las actividades de gestión de la seguridad de la información deban ser realizadas.

2.4 Proceso de autorización para nuevos servicios de procesamiento de la información

a) Asignar un custodio o responsable para cualquier nuevo servicio a implementar, generalmente del área peticionaria, incluyendo la definición de las características de la información y la definición de los diferentes niveles de acceso por usuario.

b) Autorizar explícitamente por parte del custodio el uso de un nuevo servicio según las definiciones anteriores.

c) Solicitar la autorización del oficial de seguridad de la información el uso del nuevo servicio garantizando el cumplimiento de la políticas de seguridad de la información y normas definidas en este documento.

d) Evaluar la compatibilidad a nivel de hardware y software con sistemas internos .

e) Implementar los controles necesarios para el uso de nuevos servicios para procesar información de la institución sean personales o de terceros para evitar nuevas vulnerabilidades.

2.5. Acuerdos sobre Confidencialidad (*)

a) Elaborar y aprobar los acuerdos de confidencialidad y de no-divulgación de información conforme la Constitución, las leyes, las necesidades de protección de información de la institución y el EGSI.

b) Controlar que los acuerdos de confidencialidad de la información, documento físico o electrónico, sean firmados de forma manuscrita o electrónica por todo el personal de la institución sin excepción.

c) Gestionar la custodia de los acuerdos firmados, en los expedientes, físicos o electrónicos, de cada funcionario, por parte del área de gestión de recursos humanos.

d) Controlar que la firma de los acuerdos de confidencialidad sean parte de los procedimientos de incorporación de nuevos funcionarios a la institución, sin excepción.

e) Gestionar la aceptación, entendimiento y firma de acuerdos de confidencialidad y de no divulgación de información por parte de terceros (ej., contratistas,

proveedores, pasantes, entre otros) que deban realizar labores dentro de la institución sea por medios lógicos o físicos y que involucren el manejo de información.

2.6 Contacto con las autoridades

a) Establecer un procedimiento que especifique cuándo y a cuales autoridades se reportarán incidentes derivados del infringimiento de la política de seguridad o por acciones de seguridad de cualquier origen (ej., SNAP, fiscalía, policía, bomberos, 911, otros). Todo incidente de seguridad de la información que sea considerado crítico deberá ser reportado al oficial de seguridad y este a su vez al comité de seguridad y la máxima autoridad según los casos.

b) Reportar oportunamente los incidentes identificados de la seguridad de la información a la SNAP si se sospecha de incumplimiento de la ley o que provoquen indisponibilidad o continuidad.

c) Identificar y mantener actualizados los datos de contacto de proveedores de bienes o servicios de telecomunicaciones o de acceso a la Internet para gestionar potenciales incidentes.

d) Establecer acuerdos para compartir información con el objeto de mejorar la cooperación y la coordinación de los temas de la seguridad. Tales acuerdos deberían identificar los requisitos para la protección de la información sensible.

2.7 Contactos con grupos de interés especiales

a) Mantener contacto apropiados con organizaciones públicas y privadas, asociaciones profesionales y grupos de interés especializados en seguridad de la información para mejorar el conocimiento sobre mejores prácticas y estar actualizado con información pertinente a gestión de la seguridad.

b) Recibir reportes advertencias oportunas de alertas, avisos y parches relacionados con ataques y vulnerabilidades de organizaciones públicas, privadas y académicas reconocidas por su aporte a la gestión de la seguridad de la información .

c) Establecer contactos entre oficiales y responsables de la seguridad de la información para compartir e intercambiar información acerca de nuevas tecnologías, productos, amenazas o vulnerabilidades;.

2.8 Revisión independiente de la seguridad de la información

a) Ejecutar revisiones independientes de la gestión de la seguridad a intervalos planificados o cuando ocurran cambios significativos en la implementación

b) Identificar oportunidades de mejora y la necesidad de cambios en el enfoque de la seguridad, incluyendo la política y los objetivos de control a partir de las revisiones independientes. La revisión deberá contemplar las actuaciones de la alta dirección, del comité de seguridad y del oficial de seguridad en materia de gestión de la seguridad.

c) Registrar y documentar todas las revisiones independientes de la gestión de la seguridad de la información que la institución realice.

2.9 Identificación de los riesgos relacionados con las partes externas

a) Identificar y evaluar los riesgos para la información y los servicios de procesamiento de información de la entidad en los procesos que involucran terceras partes e implementar los controles apropiados antes de autorizar el acceso.

b) Bloquear el acceso de la tercera parte a la información de la organización hasta haber implementado los controles apropiados y, cuando es viable, haber firmado un contrato que defina los términos y las condiciones del caso así como acuerdos de confidencialidad respecto de la información a la tendrán acceso.

c) Garantizar que la tercera parte es consciente de sus obligaciones y acepta las responsabilidades y deberes involucrados en el acceso, procesamiento, comunicación o gestión de la información y los servicios de procesamiento de información de la organización.

d) Registrar y mantener las terceras partes vinculadas a la entidad considerando los siguientes tipos:

- proveedores de servicios (ej., Internet, proveedores de red, servicios telefónicos, servicios de mantenimiento, energía eléctrica, agua, entre otros);
- servicios de seguridad;
- contratación externa de proveedores de servicios y/u operaciones;
- asesores y auditores externos;
- limpieza, alimentación y otros servicios de soporte contratados externamente;
- personal temporal (estudiantes, pasantes,funcionarios públicos externos);
- ciudadanos/clientes;
- Otros

2.10 Consideraciones de la seguridad cuando se trata con ciudadanos o clientes

a) Identificar requisitos de seguridad antes de facilitar servicios a ciudadanos o clientes de entidades gubernamentales que utilicen o procesen información de los mismos o de la entidad. Se podrá utilizar los siguientes criterios:

- protección de activos de información;
- descripción del producto o servicio;
- las diversas razones, requisitos y beneficios del acceso del cliente;
- política de control del acceso;
- convenios para gestión de inexactitudes de la información, incidentes de la seguridad de la información y violaciones de la seguridad;
- descripción de cada servicio que va a estar disponible;
- nivel de servicio comprometido y los niveles inaceptables de servicio;
- el derecho a monitorear y revocar cualquier actividad relacionada con los activos de la organización;
- las respectivas responsabilidades civiles de la organización y del cliente;
- las responsabilidades relacionadas con asuntos legales y la forma en que se garantiza el cumplimiento de los requisitos legales
- derechos de propiedad intelectual y asignación de derechos de copia y la protección de cualquier trabajo colaborativos
- protección de datos en base la Constitución y leyes nacionales, particularmente datos personales o financieros de los ciudadanos

2.11 Consideraciones de la seguridad en los acuerdos con terceras partes

a) Garantizar que exista un entendimiento adecuado en los acuerdos que se firmen entre la organización y la tercera parte con el objeto de cumplir los requisitos de la seguridad de la entidad. Refiérase a la norma INEN ISO/IEC para los aspectos claves a considerar en este control.

3. GESTIÓN DE LOS ACTIVOS

3.1. Inventario de activos

Inventariar los activos primarios, en formatos físicos y/o electrónicos:

a) Los procesos estratégicos, claves y de apoyo de la institución.

b) Las normas y reglamentos que son la razón de ser de la institución.

c) Planes estratégicos y operativos de la institución y áreas específicas.

d) Los archivos generados por los servidores públicos, tanto de manera física como electrónica, razón de ser de la función que desempeñan en la institución.

e) Los manuales e instructivos de sistemas informáticos: instalación, guía de usuario, operación, administración, mantenimiento, entre otros.

f) De la operación de los aplicativos informáticos de los servicios informáticos: datos y meta-datos asociados, archivos de configuración, código fuente, respaldos, versiones, etc.

g) Del desarrollo de aplicativos de los servicios informáticos: actas de levantamiento de requerimientos, documento de análisis de requerimientos, modelos entidad – relación, diseño de componentes, casos de uso, diagramas de flujo y estado, casos de prueba, etc.

h) Del soporte de aplicativos de los servicios informáticos: tickets de soporte, reportes físicos y electrónicos, evaluaciones y encuestas, libros de trabajo para capacitación, etc.

i) De la imagen corporativa de la institución: manual corporativo (que incluye manual de marca y fuentes en formato electrónico de logos), archivos multimedia, tarjetas de presentación, volantes, banners, trípticos, etc.

Inventariar los activos de soporte de Hardware (*):

j) Equipos móviles: teléfono inteligente (smartphone), teléfono celular, tableta, computador portátil, asistente digital personal (PDA), etc.

k) Equipos fijos: servidor de torre, servidor de cuchilla, servidor de rack, computador de escritorio, computadoras portátiles, etc.

l) Periféricos de entrada: teclado, ratón, micrófono, escáner plano, escáner de mano, cámara digital, cámara web, lápiz óptico, pantalla de toque, etc.

m) Periféricos de salida: monitor, proyector, audífonos, parlantes, impresora láser, impresora de inyección de tinta, impresora matricial, impresora térmica, plóter, máquina de fax, etc.

n) Periféricos y dispositivos de almacenamiento: sistema de almacenamiento (NAS, SAN), librería de cintas, cintas magnéticas, disco duro portátil, disco flexible, grabador de discos (CD, DVD, Blu-ray), CD, DVD, Blu-ray, memoria USB, etc.

o) Periféricos de comunicaciones: tarjeta USB para redes inalámbricas (Wi-Fi, Bluetooth, GPRS, HSDPA), tarjeta PCMCIA para redes inalámbricas (Wi-Fi, Bluetooth, GPRS, HSDPA), tarjeta USB para redes alámbricas/inalámbricas de datos y de telefonía, etc.

p) Tableros: de transferencia (bypass) de la unidad ininterrumpible de energía (UPS), de salidas de energía eléctrica, de transferencia automática de energía, etc.

q) Sistemas: de control de acceso, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión, etc.

Inventariar los activos de soporte de Software (*):

r) Sistemas operativos.

s) Software de servicio, mantenimiento o administración de: gabinetes de servidores de cuchilla, servidores (estanteria/rack, torre, virtuales), sistema de redes de datos, sistemas de almacenamiento (NAS, SAN), telefonía, sistemas (de UPS, grupo electrógeno, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión), etc.

t) Paquetes de software o software base de: suite de ofimática, navegador de Internet, cliente de correo electrónico, mensajería instantánea, edición de imágenes, video conferencia, servidor (proxy, de archivos, de correo electrónico, de impresiones, de mensajería instantánea, de aplicaciones, de base de datos), etc.

u) Aplicativos informáticos del negocio.

Inventariar los activos de soporte de redes (*):

v) Cables de comunicaciones (interfaces: RJ-45 o RJ-11, SC, ST o MT-RJ,interfaz V35, RS232, USB, SCSI, LPT), panel de conexión (patch panel), tomas o puntos de red, racks (cerrado o abierto, de piso o pared), etc.

w) Switchs (de centros de datos, de acceso, de borde, de gabinete de servidores, access-point, transceiver, equipo terminal de datos, etc.).

x) Ruteador (router), cortafuego (firewall), controlador de red inalámbrica, etc.

y) Sistema de detección/prevención de intrusos (IDS/IPS), firewall de aplicaciones web, balanceador de carga, switch de contenido, etc.

Inventariar los activos referentes a la estructura organizacional:

z) Estructura organizacional de la institución, que incluya todas las unidades administrativas con los cargos y nombres de las autoridades: área de la máxima autoridad, área administrativa, área de recurso humano, área financiera, etc.

aa) Estructura organizacional del área de las TIC, con los cargos y nombres del personal: administrador (de servidores, de redes de datos, de respaldos de la información, de sistemas de almacenamiento, de bases de datos, de seguridades, de aplicaciones del negocio, de recursos informáticos, etc.), líder de proyecto, personal de capacitación, personal de mesa de ayuda, personal de aseguramiento de calidad, programadores (PHP, Java, etc.).

bb) Inventario referente a los sitios y edificaciones de la institución: planos arquitectónicos, estructurales, eléctricos, sanitarios, de datos, etc.

cc) Dirección física, dirección de correo electrónico, teléfonos y contactos de todo el personal de la institución.

dd) De los servicios esenciales: número de líneas telefónicas fija y celulares, proveedor de servicios de Internet y transmisión de datos, proveedor del suministro de energía eléctrica, proveedor del suministro de agua potable, etc.

Los activos deberán ser actualizados ante cualquier modificación de la información registrada y revisados con una periodicidad no mayor a seis meses.

3.2. Responsable de los activos

a) Asignar los activos asociados (o grupos de activos) a un individuo que actuará como Responsable del Activo. Por ejemplo, debe haber un responsable de los computadores de escritorio, otro de los celulares, otro de los servidores del centro de datos, etc. El término "responsable" no implica que la persona tenga realmente los derechos de propiedad de los activos. El Responsable del Activo tendrá las siguientes funciones:

- Elaborar el inventario de los activos a su cargo y mantenerlo actualizado.
- Delegar tareas rutinarias, tomando en cuenta que la responsabilidad sigue siendo del responsable.
- Administrar la información dentro de los procesos de la institución a los cuales ha sido asignado.
- Elaborar las reglas para el uso aceptable del mismo e implantarlas previa autorización de la autoridad correspondiente.
- Clasificar, documentar y mantener actualizada la información y los activos, y definir los permisos de acceso a la información.

b) Consolidar los inventarios de los activos a cargo del Responsable del Activo, por área o unidad organizativa.

3.3. Uso aceptable de los activos

a) Identificar, documentar e implementar las reglas sobre el uso aceptable de los activos asociados con los servicios de procesamiento de la información. Para la elaboración de las reglas, el Responsable del Activo deberá tomar en cuenta las actividades definidas en los controles correspondientes a los ámbitos de "Intercambio de Información" y "Control de Acceso", donde sea aplicable.

b) El Oficial de Seguridad de la Información es el encargado de asegurar que los lineamientos para la utilización de los recursos de las Tecnologías de la

Información contemplen los requerimientos de seguridad establecidos, según la criticidad de la información que procesan.

c) La información y documentos generados en la institución y enviados por cualquier medio o herramienta electrónica son propiedad de la misma institución.

d) Reglamentar el uso de correo electrónico institucional (*):

- Este servicio debe utilizarse exclusivamente para las tareas propias de las funciones que se desarrollan en la institución y no debe utilizarse para ningún otro fin.
- Cada persona es responsable tanto del contenido del mensaje enviado como de cualquier otra información que adjunte.
- Todos los mensajes deben poder ser monitoreados y conservados permanentemente por parte de la institución.
- Toda cuenta de correo electrónico debe estar asociada a una única cuenta de usuario.
- La conservación de los mensajes se efectuará en carpetas personales, para archivar la información de acceso exclusivo del usuario y que no debe compartirse con otros usuarios. Debe definirse un límite de espacio máximo.
- Toda la información debe ser gestionada de forma centralizada y no en las estaciones de trabajo de los usuarios.
- Todo sistema debe contar con las facilidades automáticas que notifiquen al usuario cuando un mensaje enviado por él no es recibido correctamente por el destinatario, describiendo detalladamente el motivo del error.
- Deben utilizarse programas que monitoreen el accionar de virus informáticos tanto en mensajes como en archivos adjuntos, antes de su ejecución.
- Todo usuario es responsable por la destrucción de los mensajes con origen desconocido, y asume la responsabilidad por las consecuencias que pueda ocasionar la ejecución de los archivos adjuntos. En estos casos, no deben contestar dichos mensajes y deben enviar una copia al Oficial de Seguridad de la Información para que efectúe el seguimiento y la investigación necesaria.
- Para el envío y la conservación de la información, debe implementarse el cifrado (criptografía) de datos.
- Todo usuario es responsable de la cantidad y tamaño de mensajes que envíe. Debe controlarse el envío no autorizado de correos masivos.

e) Reglamentar el acceso y uso de la Internet y sus aplicaciones/servicios (*):

- Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en la institución, y no debe utilizarse para ningún otro fin.
- Cada usuario es responsable de la información y contenidos a los que accede y de aquella que copia para conservación en los equipos de la institución.
- Debe limitarse a los usuarios el acceso a portales, aplicaciones o servicios de la Internet y la Web que pudieren perjudicar los intereses y la reputación de la institución. Específicamente, se debe bloquear el acceso por medio de dispositivos fijos y/o móviles a aquellos portales, aplicaciones o servicios de la Internet y la Web sobre pornografía, racismo, violencia, delincuencia o de contenidos ofensivos y contrarios a los intereses, entre otros, y valores de la institución o que impacten negativamente en la productividad y trabajo de la institución (ej., mensajería instantánea-chats, redes sociales, video, otros) y particularmente a los que atenten a la ética y moral.
- El Oficial de Seguridad de la Información debe elaborar, poner en marcha y controlar la aplicación de un procedimiento institucional para acceso y uso de la Internet y la Web por parte de todo funcionario sin excepción, y en el cual se acepten las condiciones aquí especificadas y otras que la institución considere apropiadas.
- Todos los accesos deben poder ser sujetos de monitoreo y conservación permanente por parte de la institución.
- El Oficial de Seguridad de la Información, puede acceder a los contenidos monitoreados, con el fin de asegurar el cumplimiento de las medidas de seguridad.
- La institución podrá en cualquier momento bloquear o limitar el acceso y uso de la Internet a los funcionarios o a terceros que accedan tanto por medio alámbrico como inalámbrico.
- Se debe bloquear y prohibir el acceso y uso de servicios de correo electrónico de libre uso tales como: Gmail, Hotmail, Yahoo, Facebook, entre otros.
- Se prohíbe expresamente a las entidades de la Administración Pública la contratación, acceso y uso de servicios de correo electrónico en la Internet (Nube), para uso institucional o de servidores públicos, con empresas privadas o públicas cuyos centros de datos, redes (salvo la Internet), equipos, software base y de gestión de correo electrónico y cualquier elemento tecnológico necesario, se

encuentren fuera del territorio nacional, y adicionalmente, si las condiciones de los servicios que tales empresas prestaren no se someten a la Constitución y Leyes Ecuatorianas.

f) Reglamentar el uso de los sistemas de video-conferencia (*):

- Definir un responsable para administrar la video-conferencia.
- Definir y documentar el procedimiento de acceso a los ambiente de pruebas y producción.
- Elaborar un documento tipo "lista de chequeo" (check-list) que contenga los parámetros de seguridad para el acceso a la red interministerial que soporta el servicios de video-conferencia.
- Crear contraseñas para el ingreso a la configuración de los equipos y para las salas virtuales de video-conferencia.
- Deshabilitar la respuesta automática de los equipos de video-conferencia.

3.4. Directrices de clasificación de la información

a) Clasificar la información como pública o confidencial. (*)

b) Elaborar y aprobar un catálogo de clasificación de la información. Se la deberá clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la institución. El nivel de protección se puede evaluar analizando la confidencialidad, la integridad y la disponibilidad

3.5. Etiquetado y manejo de la información

a) Incluir datos mediante abreviaturas, acerca del tipo de activo y su funcionalidad para la generación de etiquetas.

b) En caso de repetirse la etiqueta del activo, deberá añadirse un número secuencial único al final.

c) En caso de documentos en formato electrónico, la etiqueta deberá asociarse a un metadato único, pudiendo ser éste un código MD5.

d) Las etiquetas generadas deberán estar incluidas en el inventario, asociadas a su respectivo activo.

e) Los responsables de los activos supervisarán el cumplimiento del proceso de generación de etiquetas y rotulación de los activos.

f) Para el caso de etiquetas físicas, los responsables de los activos verificarán con una periodicidad no mayor a 6 meses, que los activos se encuentren rotulados y con etiquetas legibles.

g) En caso de destrucción de un activo, la etiqueta asociada a éste debe mantenerse en el inventario respectivo con los registros de las acciones realizadas.

4. SEGURIDAD DE LOS RECURSOS HUMANOS

4.1. Funciones y responsabilidades

a) Verificar a los candidatos, previa su contratación, el certificado de antecedentes penales y revisar la información entregada en su hoja de vida (*).

b) Entregar formalmente a los funcionarios sus funciones y responsabilidades (*).

c) Notificar al Oficial de Seguridad de la Información los permisos necesarios para activación y acceso a los activos de información.

d) Informar al Oficial de Seguridad de la Información sobre los eventos potenciales, intentos de intrusión u otros riesgos que puedan afectar la seguridad de la información de la institución.

4.2 Selección

a) Verificar antecedentes de candidatos a ser empleados, contratistas o usuarios de terceras partes, o designaciones y promociones de funcionarios de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a la naturaleza y actividades de la entidad pública, a la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos. No debe entenderse este control como discriminatorio en ningún aspecto.

b) Definir los criterios y las limitaciones para las revisiones de verificación de personal actual (por motivos de designación o promoción), potenciales empleados y de terceras partes.

c) Informar del procedimiento de revisión y solicitar el consentimiento al personal actual (por motivos de designación o promoción), potenciales empleados y de terceras partes.

4.3. Términos y condiciones laborales

a) Realizar la firma de un acuerdo de confidencialidad o no-divulgación, antes de que los empleados, contratistas y usuarios de terceras partes, tengan acceso a la información. Dicho acuerdo debe establecer los parámetros tanto de vigencia del acuerdo, información confidencial referida, formas de acceso, responsabilidades y funciones.

b) Socializar los derechos y responsabilidades legales de los empleados, los contratistas y cualquier otro usuario sobre la protección de datos; dejando constancia de lo actuado a través de hojas de registro, informes o similares, que evidencie la realización de la misma.

c) Responsabilizar al personal sobre el manejo y creación de la información resultante durante el contrato laboral con la institución.

4.4. Responsabilidades de la dirección a cargo del funcionario

a) Explicar y definir las funciones y las responsabilidades respecto a la seguridad de la información, antes de otorgar el acceso a la información, contraseñas o sistemas de información sensibles (*).

b) Lograr la concienciación sobre la seguridad de la información correspondiente a sus funciones y responsabilidades dentro de la institución.

c) Acordar los términos y las condiciones laborales, las cuales incluyen la política de la seguridad de la información de la institución y los métodos apropiados de trabajo.

d) Verificar el cumplimiento de las funciones y responsabilidades respecto a la seguridad de la información mediante la utilización de reportes e informes.

4.5. Educación, formación y sensibilización en seguridad de la información

a) Socializar y capacitar de forma periódica y oportuna sobre las normas y los procedimientos para la seguridad, las responsabilidades legales y los controles de la institución, así como en la capacitación del uso correcto de los servicios de información.

4.6. Proceso disciplinario

a) Garantizar el tratamiento imparcial y correcto para los empleados que han cometido violaciones comprobadas a la seguridad de la información.

b) Considerar sanciones graduales, dependiendo de factores tales como la naturaleza, cantidad y la gravedad de la violación, así como su impacto en el negocio, el nivel de capacitación del personal, la legislación correspondiente (ej., Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, EGSI, etc.,) y otros factores existentes en los procedimientos propios de la entidad.

4.7. Responsabilidades de terminación del contrato

a) Comunicar oficialmente al personal las responsabilidades para la terminación de su relación laboral, lo cual debe incluir los requisitos permanentes para la seguridad de la información y las responsabilidades legales o contenidas en cualquier acuerdo de confidencialidad.

b) Los cambios en la responsabilidad o en el contrato laboral deberán ser gestionados como la terminación de la responsabilidad o el contrato laboral respectivo, y la nueva responsabilidad o contrato laboral se deberá instaurar en el contrato de confidencialidad respectivo.

c) Previa la terminación de un contrato se deberá realizar la transferencia de la documentación e información de la que fue responsable al nuevo funcionario a cargo, en caso de ausencia, al Oficial de Seguridad de la Información.

d) Los contratos del empleado, el contratista o el usuario de terceras partes, deben incluir las responsabilidades válidas aún después de la terminación del contrato laboral.

4.8. Devolución de activos

a) Formalizar el proceso de terminación del contrato laboral, para incluir la devolución de software, documentos corporativos y los equipos. También es necesaria la devolución de otros activos de la institución tales como los dispositivos de cómputo móviles, tarjetas de crédito, las tarjetas de acceso, tokens USB con certificados de electrónicos, certificados electrónicos en archivo, memorias flash, teléfonos celulares, cámaras, manuales, información almacenada en medios electrónicos y otros estipulados en las políticas internas de cada entidad.

b) Aplicar los debidos procesos para garantizar que toda la información generada por el empleado, contratista o usuario de terceras partes dentro de la institución, sea transferida, archivada o eliminada con seguridad.

c) Realizar el proceso de traspaso de conocimientos por parte del empleado, contratistas o terceras partes, luego de la terminación de su contrato laboral, para la continuación de las operaciones importantes dentro de la institución.

4.9. Retiro de los privilegios de acceso

a) Retirar los privilegios de acceso a los activos de información y a los servicios de procesamiento de información (ej., sistema de directorio, correo electrónico, accesos físicos, aplicaciones de software, etc.,) inmediatamente luego de que se comunique formalmente al Oficial de Seguridad de la Información formalmente la terminación de la relación laboral por parte del área correspondiente.

5. SEGURIDAD FÍSICA Y DEL ENTORNO

5.1. Perímetro de la seguridad física

a) Definir y documentar claramente los perímetros de seguridad (barreras, paredes, puertas de acceso controladas con tarjeta, etc.), con una ubicación y fortaleza adecuadas.

b) Definir una área de recepción, con personal y otros medios para controlar el acceso físico al lugar o edificio (*).

c) Extender las barreras físicas necesarias desde el piso hasta el techo a fin de impedir el ingreso inapropiado y la contaminación del medio ambiente.

d) Disponer de alarmas de incendio y puertas de evacuación debidamente monitoreadas que cumplan normas nacionales e internacionales.

e) Disponer de un sistema de vigilancia mediante el uso de circuitos cerrados de televisión.

f) Aislar los ambientes de procesamiento de información de los ambientes proporcionados por terceros.

5.2. Controles de acceso físico

a) Supervisar la permanencia de los visitantes en las áreas restringidas y registrar la hora y fecha de su ingreso y salida (*).

b) Controlar y limitar el acceso, exclusivamente a personal autorizado, a la información clasificada y a las instalaciones de procesamiento de información. Se debe utilizar controles de autenticación como tarjetas de control de acceso más el número de identificación personal.

c) Implementar el uso de una identificación visible para todo el personal y visitantes, quienes deberán ser escoltados por una persona autorizada para el tránsito en las áreas restringidas (*).

d) Revisar y actualizar periódicamente los derechos de acceso a las áreas restringidas, mismos que serán documentados y firmados por el responsable.

5.3. Seguridad de oficinas, recintos e instalaciones

a) Aplicar los reglamentos y las normas en materia de sanidad y seguridad.

b) Proteger las instalaciones claves de tal manera que se evite el acceso al público (*).

c) Establecer que los edificios o sitios de procesamiento sean discretos y tengan un señalamiento mínimo apropiado.

d) Ubicar las impresoras, copiadoras, etc., en un área protegida(*).

e) Disponer que las puertas y ventanas permanezcan cerradas, especialmente cuando no haya vigilancia.

5.4. Protección contra amenazas externas y ambientales.

a) Almacenar los materiales combustibles o peligrosos a una distancia prudente de las áreas protegidas.

b) Ubicar los equipos de repuesto y soporte a una distancia prudente para evitar daños en caso de desastre que afecte las instalaciones principales.

c) Suministrar el equipo apropiado contra incendios y ubicarlo adecuadamente.

d) Realizar mantenimientos de las instalaciones eléctricas y UPS.(*)

e) Realizar mantenimientos en los sistemas de climatización y ductos de ventilación (*).

f) Adoptar controles para minimizar el riesgo de amenazas físicas potenciales como robo, incendio, explosión, humo, agua, polvo, vibración, efectos químicos, interferencia del suministro eléctrico e interferencia a las comunicaciones.

5.5. Trabajo en áreas seguras

a) Dar a conocer al personal, la existencia de un área segura.

b) Evitar el trabajo no supervisado para evitar actividades maliciosas.

c) Revisar periódicamente y disponer de un bloqueo físico de las áreas seguras vacías.

d) No permitir equipos de grabación, cámaras, equipos de video y audio, dispositivos móviles, etc., a menos de que estén autorizados (*).

5.6. Áreas de carga, despacho y acceso público

a) Permitir el acceso al área de despacho y carga, únicamente a personal identificado y autorizado (*).

b) Descargar y despachar los suministros, únicamente en el área de descarga y despacho.

c) Asegurar las puertas externas e internas de despacho y carga.

d) Inspeccionar el material que llega para determinar posibles amenazas.

e) Registrar el material que llega, de acuerdo a los procedimientos de gestión de activos.

5.7. Ubicación y protección de los equipos

a) Ubicar los equipos de modo que se elimine el acceso innecesario a las áreas de trabajo restringidas.

b) Aislar los servicios de procesamiento de información con datos sensibles y elementos que requieran protección especial, para reducir el riesgo de visualización de la información de personas no autorizadas.

c) Establecer directrices para no comer, beber y fumar en las cercanías de las áreas de procesamiento de información (*).

d) Monitorear las condiciones ambientales de temperatura y humedad.

e) Tener protección contra descargas eléctricas en todas las edificaciones de la institución y disponer de filtros protectores en el suministro de energía y en las líneas de comunicación.

f) Disponer de métodos especiales de protección para equipos en ambientes industriales.

5.8. Servicios de suministro

a) Implementar y documentar los servicios de electricidad, agua, calefacción, ventilación y aire acondicionado, suministrados a la institución.

b) Inspeccionar regularmente todos los sistemas de suministro.

c) Tener un sistema de suministro de energía sin interrupción (UPS) o al menos permitir el cierre/apagado ordenado de los servicios y equipos que soportan las operaciones críticas de los servicios informáticos de la institución (*).

d) Tener al alcance el suministro de combustible para que el grupo electrógeno pueda funcionar mientras dure la suspensión del suministro eléctrico público.

e) Disponer de los interruptores de emergencia cerca de las salidas, para suspender el paso de energía eléctrica, en caso de un incidente o problema.

5.9. Seguridad del cableado

a) Disponer de líneas de fuerza (energía) y de telecomunicaciones subterráneas protegidas, en cuanto sea posible.

b) Proteger el cableado de la red contra la intercepción o daño.

c) Separar los cables de energía de los cables de comunicaciones.

d) Identificar y rotular los cables de acuerdo a normas locales o internacionales para evitar errores en el manejo.

e) Disponer de documentación, diseños/planos y la distribución de conexiones de: datos alámbricas/inalámbricas (locales y remotas), voz, eléctricas polarizadas, etc. (*).

f) Controlar el acceso a los módulos de cableado de conexión (patch panel) y cuartos de cableado.

5.10. Mantenimiento de los equipos

a) Brindar mantenimientos periódicos a los equipos y dispositivos, de acuerdo a las especificaciones y recomendaciones del proveedor.

b) Realizar el mantenimiento de los equipos únicamente con personal calificado y autorizado.

c) Conservar los registros de los mantenimientos preventivos, correctivos y fallas relevantes o sospechosas.

d) Establecer controles apropiados para realizar mantenimientos programados y emergentes.

e) Gestionar mantenimientos planificados con hora de inicio, fin, impacto y responsables y poner previamente en conocimiento de administradores y usuarios finales.

5.11. Seguridad de los equipos fuera de las instalaciones

a) Custodiar los equipos y medios que se encuentren fuera de las instalaciones de la institución. Tomar en cuenta las instrucciones del fabricante para la protección de los equipos que se encuentren fuera de estas instalaciones.

b) Disponer de controles para el trabajo que se realiza en equipos fuera de las instalaciones, mediante una evaluación de riesgos.

c) Establecer una cobertura adecuada del seguro, para proteger los equipos que se encuentren fuera de las instalaciones.

5.12. Seguridad en la reutilización o eliminación de los equipos

a) Destruir, borrar o sobrescribir los dispositivos que contienen información sensible utilizando técnicas que permiten la no recuperación de la información original.

b) Evaluar los dispositivos deteriorados que contengan información sensible antes de enviar a reparación, borrar la información o determinar si se debería eliminar físicamente el dispositivo.

5.13. Retiro de activos de la propiedad

a) Tener autorización previa para el retiro de cualquier equipo, información o software.

b) Identificar a los empleados, contratistas y usuarios de terceras partes, que tienen la autorización para el retiro de activos de la institución.

c) Establecer límites de tiempo para el retiro de equipos y verificar el cumplimiento en el momento de la devolución.

d) Registrar cuando el equipo o activo sea retirado y cuando sea devuelto.

6. GESTIÓN DE COMUNICACIONES Y OPERACIONES

6.1. Documentación de los procedimientos de Operación

a) Documentar el procesamiento y manejo de la información.

b) Documentar el proceso de respaldo y restauración de la información.

c) Documentar todos los procesos de los servicios de procesamiento de datos, incluyendo la interrelación con otros sistemas.

d) Documentar las instrucciones para el manejo de errores y otras condiciones excepcionales que pueden surgir durante la ejecución de las tareas.

e) Documentar los contactos de soporte, necesarios en caso de incidentes (*).

f) Documentar las instrucciones para el manejo de medios e informes especiales, incluyendo procedimientos para la eliminación segura de informes de tareas fallidas.

g) Documentar los procedimientos para reinicio y recuperación del sistema en caso de fallas.

h) Documentar los registros de auditoría y de la información de registro del sistema.

6.2. Gestión del Cambio

a) Identificar y registrar los cambios significativos.

b) Evaluar el impacto de dichos cambios.

c) Aprobar de manera formal los cambios propuestos.

d) Planificar el proceso de cambio.

e) Realizar pruebas del cambio.

f) Comunicar el detalle de cambios a todas las personas involucradas.

g) Identificar responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

h) Establecer responsables y procedimientos formales del control de cambios en los equipos y software. Los cambios deben efectuarse únicamente cuando haya razón válida para el negocio, como: cambio de versión, corrección de vulnerabilidades, costos, licenciamiento, nuevo hardware, etc.

6.3. Distribución de funciones

a) Distribuir las funciones y las áreas de responsabilidad, para reducir oportunidades de modificaciones no autorizadas, no intencionales, o el uso inadecuado de los activos de la institución.

b) Limitar el acceso a modificar o utilizar los activos sin su respectiva autorización.

c) Establecer controles de monitoreo de actividades, registros de auditoría y supervisión por parte de la dirección.

6.4. Separación de las instancias de Desarrollo, Pruebas, Capacitación y Producción.

a) Definir y documentar diferentes entornos para desarrollo, pruebas, capacitación y producción. Para el caso que no se pueda definir diferentes entornos con recursos físicos independientes, se debe mantener diferentes directorios con su respectiva versión y delegación de acceso.

b) Aislar los ambientes de desarrollo, pruebas, capacitación y producción.

c) Controlar la instalación y uso de herramientas de desarrollo de software y/o acceso a bases de datos y redes en los equipos informáticos, salvo que sean parte de las herramientas de uso estándar o su instalación sea autorizada de acuerdo a un procedimiento expresamente definido.

d) Implantar ambientes de prueba, iguales en capacidad, a los ambientes de producción.

e) Utilizar sistemas de autenticación y autorización independientes para las diversas instancias o ambientes.

f) Definir perfiles de usuario para las diferentes instancias o ambientes.

g) Aislar los datos sensibles de los ambientes de desarrollo, pruebas y capacitación

h) Permitir al personal de desarrollo de software el acceso al entorno de producción, únicamente en caso de extrema necesidad, con la autorización explícita correspondiente.

6.5. Presentación del Servicio.

a) Establecer controles sobre definiciones del servicio y niveles de prestación del servicio, para que sean implementados, mantenidos y operados por terceros.

b) Establecer controles de cumplimiento de terceros, que garanticen la capacidad de servicio, planes ejecutables y diseños para la continuidad del negocio, en caso de desastres.

6.6. Monitoreo y revisión de los servicios, por terceros.

a) Identificar los sistemas sensibles o críticos que convenga tener dentro o fuera de la institución.

b) Monitorear los niveles de desempeño de los servicios para verificar el cumplimiento de los acuerdos (*).

c) Analizar los reportes de servicios, reportes de incidentes elaborados por terceros y acordar reuniones periódicas según los acuerdos (*).

d) Revisar y verificar los registros y pruebas de auditoría de terceros, con respecto a eventos de seguridad, problemas de operación, fallas relacionados con el servicio prestado (*).

6.7. Gestión de los cambios en los servicios ofrecidos por terceros.

a) Establecer un proceso de gestión de cambios en los servicios ofrecidos por terceros, en el desarrollo de aplicaciones, provisión de servicios de hardware, software, redes, otros.

b) Coordinar el proceso de cambio cuando se necesite realizar cambios o mejoras a las redes y uso de nuevas tecnologías en los servicios ofrecidos por terceros.

c) Coordinar el proceso de cambio cuando se realice cambio de proveedores, cambio de ubicación física en los servicios ofrecidos por terceros.

6.8. Gestión de la capacidad

a) Realizar proyecciones de los requerimientos de capacidad futura de recursos para asegurar el desempeño de los servicios y sistemas informáticos (*).

b) Monitorear los recursos asignados para garantizar la capacidad y rendimiento de los servicios y sistemas informáticos.

c) Utilizar la información del monitoreo para la adquisición, asignación de recursos y evitar cuellos de botella.

6.9. Aceptación del Sistema.

a) Verificar el desempeño y los requerimientos de cómputo necesarios para los nuevos sistemas.

b) Considerar procedimientos de recuperación y planes de contingencia.

c) Poner a prueba procedimientos operativos de rutina según normas definidas para el sistema.

d) Garantizar la implementación de un conjunto de controles de seguridad acordados.

e) Asegurar que la instalación del nuevo sistema no afecte negativamente los sistemas existentes, especialmente en períodos pico de procesamiento.

f) Considerar el efecto que tiene el nuevo sistema en la seguridad global de la institución.

g) Capacitar sobre el funcionamiento y utilización del nuevo sistema.

h) Para nuevos desarrollos, se debe involucrar a los usuarios y a todas las áreas relacionadas, en todas las fases del proceso, para garantizar la eficacia operativa del sistema propuesto.

6.10. Controles contra código malicioso.

a) Prohibir el uso de software no autorizado por la institución. Elaborar un listado del software autorizado. (*).

b) Establecer procedimientos para evitar riesgos en la obtención/descarga de archivos y software desde o a través de redes externas o por cualquier otro medio.

c) Instalar y actualizar periódicamente software de antivirus y contra código malicioso (*).

d) Mantener los sistemas operativos y sistemas de procesamiento de información actualizados con las últimas versiones de seguridad disponibles (*).

e) Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la institución.

f) Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos o en archivos recibidos a través de redes no confiables.

g) Redactar procedimientos para verificar toda la información relativa a software malicioso.

h) Emitir boletines informativos de alerta con información precisa.

i) Concienciar al personal acerca del problema de los virus y cómo proceder frente a los mismos.

j) Contratar con el proveedor de Internet o del canal de datos los servicios de filtrado de: virus, spam, programas maliciosos (malware), en el perímetro externo.

6.11. Controles contra códigos móviles

a) Aislar de forma lógica los dispositivos móviles en forma similar a lo que ocurre con las VLANs.

b) Bloquear códigos móviles no autorizados.

c) Gestionar el código móvil mediante procedimientos de auditoría y medidas técnicas disponibles.

d) Establecer controles criptográficos para autenticar de forma única el código móvil.

6.12. Respaldo de la información.

a) Los responsables del área de Tecnologías de la Información, Oficial de Seguridad de la Información junto con el propietario de la información, determinarán los procedimientos para el resguardo y contención de la información (*).

b) Definir el procedimiento de etiquetado de las copias de respaldo, identificando su contenido, periodicidad y retención (*).

c) Definir la extensión (completo/diferencial) y la frecuencia de los respaldos, de acuerdo a los requisitos del negocio de la institución (*).

d) Establecer procedimientos de los medios de respaldo, una vez concluida su vida útil recomendada por el proveedor y la destrucción de estos medios.

e) Guardar los respaldos en un sitio lejano, a una distancia suficiente para evitar cualquier daño debido a desastres en la sede principal de la institución.

f) Proporcionar un grado apropiado de protección física y ambiental.

g) Establecer procedimientos regulares de verificación y restauración de los medios de respaldo para garantizar sean confiables para uso de emergencia.

h) Proteger la información confidencial por medio de encriptación.

i) Considerar los respaldos a discos y en el mismo sitio si se tiene suficientes recursos, ya que en caso de mantenimientos de los sistemas de información, es más rápida su recuperación.

6.13. Controles de las redes.

a) Separar el área de redes del área de operaciones, cuando la capacidad y recursos lo permitan.

b) Designar procedimientos y responsabilidades para la gestión de equipos remotos como el caso de re-direccionamiento de puertos y accesos por VPNs, incluyendo el área de operaciones y el área de usuarios finales.

c) Establecer controles especiales para salvaguardar la confidencialidad y la integridad de los datos que pasan por las redes públicas, redes locales o inalámbricas; así como la disponibilidad de las redes.

d) Garantizar la aplicación de los controles mediante actividades de supervisión.

e) Disponer de un esquema de red de los enlaces de datos, Internet y redes locales, así como la documentación respectiva.

6.14. Seguridad de los servicios de la red.

a) Incorporar tecnología para la seguridad de los servicios de red como la autenticación, encriptación y controles de conexión de red (*).

b) Implementar soluciones que proporcionen valor agregado a las conexiones y servicios de red, como la implementación de firewalls, antivirus, etc. (*)

c) Definir procedimientos para la utilización de los servicios de red para restringir el acceso a los servicios de red cuando sea necesario.

6.15. Gestión de los medios removibles.

a) Establecer un procedimiento para la gestión de todos los medios removibles.

b) Tener autorización para la conexión de los medios removibles y registrar la conexión y retiro, para pruebas de auditoría.

c) Almacenar los medios removibles en un ambiente seguro, según las especificaciones de los fabricantes.

d) Evitar la pérdida de información por deterioro de los medios.

6.16. Eliminación de los medios

a) Identificar los medios que requieran eliminación segura.

b) Almacenar y eliminar de forma segura los medios que contengan información sensible, como la incineración, trituración o borrado de los datos.

c) Establecer procedimientos para selección del contratista que ofrece servicios de recolección y eliminación del papel, equipos y medios.

d) Registrar la eliminación de los medios para mantener pruebas de auditoría.

6.17. Procedimientos para el manejo de la información

a) Establecer procedimientos para el manejo y etiquetado de todos los medios de acuerdo a su nivel de clasificación.

b) Establecer controles de acceso para evitar el acceso de personal no autorizado.

c) Tener un registro actualizado de los receptores de los medios.

d) Establecer controles de protección según el nivel de sensibilidad de los datos que reside en la memoria temporal.

e) Almacenar los medios según especificaciones del fabricante.

6.18. Seguridad de la documentación del sistema.

a) Guardar con seguridad toda la documentación de los sistemas informáticos.

b) Mantener una lista de acceso mínima a la documentación del sistema y con su debida autorización.

c) Mantener una protección adecuada de la documentación del sistema expuesta en la red pública.

6.19. Políticas y procedimientos para el intercambio de información.

a) Establecer procedimientos para proteger la información intercambiada contra la interpretación, copiado, modificación, enrutamiento y destrucción.

b) Definir procedimientos para detección y protección contra programas maliciosos, cuando se utilizan comunicaciones electrónicas.

c) Proteger la información sensible que se encuentra en forma de adjunto.

d) Establecer directrices para el uso de los servicios de comunicación electrónica.

e) Definir procedimientos para el uso de las redes inalámbricas en base a los riesgos involucrados.

f) Establecer responsabilidades de empleados, contratistas y cualquier otro usuario de no comprometer a la institución con un mal uso de la información.

g) Establecer controles por medio de técnicas criptográficas.

h) Definir directrices de retención y eliminación de la correspondencia incluyendo mensajes, según la normativa legal local.

i) No dejar información sensible en copiadoras, impresoras, fax, contestadores, etc.

j) No revelar información sensible al momento de tener una conversación telefónica o mantener conversaciones sin tomar los controles necesarios.

k) No dejar datos demográficos al alcance de cualquier persona, como los correos electrónicos, ya que se puede hacer uso de ingeniería social para obtener más información.

6.20. Acuerdos para el intercambio

a) Definir procedimientos y responsabilidades para el control y notificación de transmisiones, envíos y recepciones.

b) Establecer procedimientos para garantizar la trazabilidad y el no repudio.

c) Definir normas técnicas para el empaquetado y transmisión.

d) Definir pautas para la identificación del prestador de servicio de correo.

e) Establecer responsabilidades y obligaciones en caso de pérdida de datos.

f) Utilizar un sistema para rotulado de la información clasificada.

g) Conocer los términos y condiciones de las licencias de software privativo o suscripciones de software de código abierto bajo las cuales se utiliza el software.

h) Conocer sobre la propiedad de la información y las condiciones de uso.

i) Definir procedimientos técnicos para la grabación y lectura de la información y del software en el intercambio de información.

6.21. Medios físicos en tránsito

a) Utilizar transporte confiable o servicios de mensajería.

b) Establecer una lista de mensajería aprobada por la dirección

c) Definir procedimientos para identificar los servicios de mensajería.

d) Embalar de forma segura medios o información enviada a través de servicios de mensajería, siguiendo las especificaciones del proveedor o del fabricante.

e) Adoptar controles especiales cuando sea necesario proteger información sensible, su divulgación y modificación.

6.22. Mensajería electrónica

a) Establecer lineamientos para proteger los mensajes contra los accesos no autorizados, modificación o denegación de los servicios.

b) Supervisar que la dirección y el transporte de mensajes sean correctos.

c) Tomar en cuenta consideraciones legales como la de firmas electrónicas.

d) Encriptar los contenidos y/o información sensibles que puedan enviarse por mensajería electrónica; utilizando firmas electrónicas reconocidas por el Estado Ecuatoriano u otras tecnologías evaluadas y aprobadas por la entidad o el Gobierno Nacional.

e) Monitorear los mensajes de acuerdo al procedimiento que establezca la institución.

6.23. Sistemas de información del negocio.

a) Proteger o tener en cuenta las vulnerabilidades conocidas en los sistemas administrativos, financieros, y demás sistemas informáticos donde la información es compartida.

b) Proteger y tener en cuenta las vulnerabilidades en los sistemas de comunicación del negocio como la grabación de las llamadas telefónicas.

c) Establecer políticas y controles adecuados para gestionar la forma en que se comparte la información.

d) Categorizar la información sensible y documentos clasificados.

e) Implementar controles de acceso a la información como acceso a proyectos confidenciales.

f) Categorizar al personal, contratistas y usuarios que tengan acceso a los sistemas informáticos y los sitios desde cuales pueden acceder.

g) Identificar el estado de las cuentas de usuario.

h) Verificar la retención y copias de respaldo de la información contenida en los sistemas informáticos.

i) Establecer requisitos y disposiciones para los recursos de emergencia.

6.24. Transacciones en línea.

a) Definir procedimientos para el uso de certificados de firmas electrónicas por las partes implicadas en la transacción.

b) Establecer procedimientos para garantizar todos los aspectos en la transacción como credenciales de usuario, confidencialidad de la transacción y privacidad de las partes.

c) Cifrar o encriptar el canal de comunicaciones entre las partes involucradas (por ejemplo, utilizando SSL/TLS).

d) Establecer protocolos seguros en la comunicación de las partes involucradas por ejemplo, utilizando SSL/TLS).

e) Establecer procedimientos para que las transacciones se encuentren fuera del entorno de acceso público.

f) Utilizar los servicios de una entidad certificadora confiable.

6.25. Información disponible al público.

a) Establecer controles para que la información disponible al público se encuentre conforme a la normativa vigente.

b) Definir controles para que la información de entrada sea procesada completamente y de forma oportuna.

c) Establecer procedimientos para que la información sensible sea protegida durante la recolección, procesamiento y almacenamiento.

6.26. Registros de auditorías.

a) Identificar el nombre de usuario.

b) Registrar la fecha, hora y detalles de los eventos clave, como registro de inicio y registro de cierre.

c) Registrar la terminal si es posible.

d) Registrar los intentos aceptados y rechazados de acceso al sistema.

e) Registrar los cambios de la configuración.

f) Registrar el uso de privilegios.

g) Registrar el uso de las aplicaciones y sistemas.

h) Registrar los accesos y tipos de acceso (*).

i) Registrar las direcciones y protocolos de red (*).

j) Definir alarmas originadas por el sistema de control de acceso(*).

k) Activación y desactivación de los sistemas de protección como antivirus y los sistemas de detección de intrusos (IDS) (*).

6.27. Monitoreo de uso del sistema.

a) Registrar los accesos autorizados, incluyendo(*):

- Identificación del ID de usuario;
- Fecha y hora de eventos clave;
- Tipos de evento;
- Archivos a los que se han tenido acceso;
- Programas y utilitarios utilizados;

b) Monitorear las operaciones privilegiadas, como (*):

- Uso de cuentas privilegiadas;
- Encendido y detección del sistema;
- Acople y desacople de dispositivos de entrada;

c) Monitorear intentos de acceso no autorizados, como (*):

- Acciones de usuario fallidas o rechazadas;
- Violación de la política de acceso y notificaciones de firewalls y gateways;
- Alertas de los sistemas de detección de intrusos;

d) Revisar alertas o fallas del sistema, como (*):

- Alertas y/o mensajes de consola;
- Excepciones de registro del sistema;
- Alarmas de gestión de red;
- Alarmas del sistema de control de acceso;

e) Revisar cambios o intentos de cambio en la configuración y los controles de la seguridad del sistema.

6.28. Protección del registro de la información.

a) Proteger de alteraciones en todos los tipos de mensaje que se registren.

b) Proteger archivos de registro que se editen o se eliminen.

c) Precautelar la capacidad de almacenamiento que exceda el archivo de registro.

d) Realizar respaldos periódicos del registro del servicio.

6.29. Registros del administrador y del operador.

a) Incluir al registro, la hora en la que ocurrió el evento (*).

b) Incluir al registro, información sobre el evento (*).

c) Incluir al registro, la cuenta de administrador y operador que estuvo involucrado (*).

d) Añadir al registro, los procesos que estuvieron implicados (*).

6.30. Registro de fallas

a) Revisar los registros de fallas o errores del sistema (*).

b) Revisar las medidas correctivas para garantizar que no se hayan vulnerado los controles (*).

c) Asegurar que el registro de fallas esté habilitado (*).

6.31 Sincronización de relojes

a) Sincronizar los relojes de los sistemas de procesamiento de información pertinentes con una fuente de tiempo exacta (ejemplo el tiempo coordinado universal o el tiempo estándar local). En lo posible, se deberá sincronizar los relojes en base a un protocolo o servicio de tiempo de red para mantener todos los equipos sincronizados.

b) Verificar y corregir cualquier variación significativa de los relojes sobretodo en sistemas de procesamiento donde el tiempo es un factor clave.

c) Garantizar que la marca de tiempo refleja la fecha/hora real considerando especificaciones locales (por ejemplo, el horario de Galápagos o de países en donde existen representación diplomáticas del país, turistas extranjeros, entre otros).

d) Garantizar la configuración correcta de los relojes para la exactitud de los registros de auditoría o control de transacciones y evitar repudio de las mismas debido a aspectos del tiempo.

7. CONTROL DE ACCESO

7.1. Política de control de acceso

a) Gestionar los accesos de los usuarios a los sistemas de información, asegurando el acceso de usuarios autorizados y previniendo los accesos no autorizados.

b) Definir responsabilidades para identificar, gestionar y mantener perfiles de los custodios de información.

c) Definir claramente los autorizadores de los permisos de acceso a la información.

7.2. Registro de usuarios

a) Establecer un procedimiento formal, documentado y difundido, en el cual se evidencie detalladamente los pasos y responsables para:

- Definir el administrador de accesos que debe controlar los perfiles y roles;
- Gestionar el documento de requerimiento de accesos de los usuarios tanto internos como externos, que contemple: el solicitante del

requerimiento o iniciador del proceso, validación del requerimiento, autorizador del requerimiento, ejecutor del requerimiento, forma y medio de entrega del acceso al usuario (manteniendo confidencialidad);

- Crear los accesos para los usuarios, para lo cual la institución debe generar convenios de confidencialidad y responsabilidad con el usuario solicitante; además, validar que el usuario tenga los documentos de ingreso con Recursos Humanos (o quien haga estas funciones) en orden y completos.

- Modificar los accesos de los usuarios;

- Eliminar los accesos de los usuarios;

- Suspender temporalmente los accesos de los usuarios en caso de vacaciones, comisiones, licencias, es decir, permisos temporales;

- Proporcionar accesos temporales a usuarios externos o terceros de acuerdo al tiempo de su permanencia y limitados según las actividades para las que fueron contratados y firmar un convenio de confidencialidad;

- Mantener un registro de la gestión de accesos a aplicaciones, redes, que evidencie, fecha de creación, eliminación, suspensión, activación o eliminación del acceso; al igual que de cada usuario, disponer de los permisos de acceso que han sido asignados.

7.3. Gestión de privilegios

a) Controlar la asignación de privilegios a través de un proceso formal de autorización.

b) Mantener un cuadro de identificación de los usuarios y sus privilegios asociados con cada servicio o sistema operativo, sistema de gestión de base de datos y aplicaciones.

c) Evidenciar documentadamente que cada activo de información tecnológico tenga definido los niveles de acceso basados en perfiles y permisos, a fin de determinar que privilegios se deben asignar según las actividades de los usuarios y la necesidad de la institución y su función.

7.4. Gestión de contraseñas para usuarios

a) Establecer un proceso formal para la asignación y cambio de contraseñas (*).

7.5. Revisión de los derechos de acceso de los usuarios

a) Realizar las depuraciones respectivas de los accesos de los usuarios, determinando un periodo máximo de 30 días; en caso de presentar cambios estructurales, esta gestión deberá hacerse inmediatamente que se ejecute el cambio organizacional.

b) Evidenciar los cambios sobre los derechos de acceso en archivos de log o registro de los sistemas, los cuales deben estar disponibles en caso que se requieran.

7.6. Uso de contraseñas

a) Documentar, en el procedimiento de accesos, las responsabilidades de los usuarios tanto internos como externos, sobre el uso de la cuenta y la contraseña asignados (*).

b) Recomendar la generación de contraseñas con letras mayúsculas, minúsculas, con caracteres especiales, difíciles de descifrar, es decir, que cumplen una complejidad media y alta (*).

c) Evitar contraseñas en blanco o que viene por defecto según el sistema el fabricante del producto, puesto que son fácilmente descifrables; por ejemplo: admin, administrador, administrador, user, usuario, entre otros (*).

d) Controlar el cambio periódico de contraseñas de los usuarios (*).

e) Generar y documentar revisiones periódicas de la gestión de usuarios incluidos los administradores de tecnología, por parte del Oficial de Seguridad de la Información (*).

7.7. Equipo de usuario desatendido

a) Implementar medidas para que, en un determinado tiempo (ej., no mayor a 10 minutos), si el usuario no está realizando ningún trabajo en el equipo, este se bloquee, y se desbloquee únicamente si el usuario ingresa nuevamente su clave (*).

7.8. Política de puesto de trabajo despejado y pantalla limpia

a) El Oficial de Seguridad de la Información deberá gestionar actividades periódicas (una vez cada mes como mínimo) para la revisión al contenido de las pantallas de los equipos, con el fin de que no se encuentren iconos y accesos innecesarios, y carpetas y archivos que deben ubicarse en la carpeta de documentos del usuario.

b) Mantener bajo llave la información sensible (cajas fuertes o gabinetes), en especial cuando no están en uso y no se encuentre personal en la oficina (*).

c) Desconectar de la red, servicio o sistema, las computadoras personales, terminales, impresoras asignadas a funciones críticas, cuando se encuentren desatendidas. Por ejemplo, haciendo uso de protectores de pantalla con clave (*).

d) Proteger los puntos de recepción de correo y fax cuando se encuentren desatendidos.

e) Bloquear las copiadoras y disponer de un control de acceso especial para horario fuera de oficinas (*).

f) Retirar información sensible una vez que ha sido impresa (*).

g) Retirar información sensible, como las claves, de sus escritorios y pantallas (*).

h) Retirar los dispositivos removibles una vez que se hayan dejado de utilizar (*).

i) Cifrar los discos duros de los computadores personales (escritorio, portátiles, etc.) y otros dispositivos que se considere necesarios, de las máximas autoridades de la institución.

7.9. Política de uso de los servicios de red

a) Levantar un registro de los servicios de red la institución.

b) Identificar por cada servicio los grupos de usuarios que deben acceder.

c) Definir los perfiles y roles para cada grupo de usuarios que tenga acceso a la red y sus servicios.

d) Definir mecanismos de bloqueos para que sea restringido el acceso de equipos a la red.

7.10. Autenticación de usuarios para conexiones externas

a) Generar mecanismos para asegurar la información transmitida por los canales de conexión remota, utilizando técnicas como encriptación de datos, implementación de redes privadas virtuales (VPN) y Servicio de Acceso Remoto (SAR) (*).

b) Realizar un mecanismo diferenciado para la autenticación de los usuarios que requieren conexiones remotas, que permita llevar control de registros (logs) y que tenga limitaciones de accesos en los segmentos de red.

7.11. Identificación de los equipos en las redes

a) Identificar y documentar los equipos que se encuentren en las redes (*).

b) Controlar que la comunicación solo sea permitida desde un equipo o lugar específico.

c) Tener documentada la identificación de los equipos que están permitidos, según la red que le corresponda.

d) Utilizar métodos para que la identificación del equipo esté en relación a la autenticación del usuario.

7.12. Protección de los puertos de configuración y diagnóstico remoto

a) Establecer un procedimiento de soporte, en el cual se garantice que los puertos de diagnóstico y configuración sean sólo accesibles mediante un acuerdo entre el administrador del servicio de computador y el personal de soporte de hardware/ software que requiere el acceso.

b) Los puertos, servicios (ej., ftp) que no se requieren por necesidades de la institución, deberán ser eliminados o deshabilitados (*).

7.13. Separación en las redes

a) Realizar una evaluación de riesgos para identificar los segmentos de red donde se encuentren los activos críticos para la institución (*).

b) Dividir las redes en dominios lógicos de red, dominio de red interna, dominio de red externa e inalámbrica.

c) Documentar la segregación de red, identificando las direcciones IP que se encuentran en cada segmento de red.

d) Configurar la puerta de enlace (gateway) para filtrar el tráfico entre dominios y bloquear el acceso no autorizado.

e) Controlar los flujos de datos de red usando las capacidades de enrutamiento/conmutación (ej., listas de control de acceso).

f) La separación de las redes debe ejecutarse en base a la clasificación de la información almacenada o procesada en la red, considerando que el objetivo es dar mayor protección a los activos de información críticos en función del riesgo que éstos podrían presentar.

g) Separar redes inalámbricas procedentes de redes internas y privadas, para evitar el acceso a terceros y de usuarios externos a las redes privadas internas.

7.14. Control de conexión a las redes

a) Restringir la capacidad de conexión de los usuarios, a través de puertas de enlace de red (gateway) que filtren el tráfico por medio de tablas o reglas predefinidas, conforme a los requerimientos de la institución.

b) Aplicar restricciones considerando:

- Mensajería
- Transferencia de archivos
- Acceso interactivo

- Acceso a las aplicaciones
- Horas del día y fechas de mayor carga

c) Incorporar controles para restringir la capacidad de conexión de los usuarios a redes compartidas especialmente de los usuarios externos a la institución.

7.15. Control del enrutamiento en la red

a) Configurar políticas de control de acceso para el enrutamiento en la red, basándose en los requerimientos de la institución (*).

Las puertas de enlace de la seguridad (gateway) se pueden usar para validar la dirección fuente/destino en los puntos de control de las redes internas y externas, si se emplean tecnologías proxy y/o de traducción de direcciones de red.

Las instituciones que utilizan proxys y quienes definen las listas de control de acceso (LCA), deben estar conscientes de los riesgos en los mecanismos empleados, a fin de que no existan usuarios o grupos de usuarios con salida libre y sin control, en base a las políticas de la institución.

7.16. Procedimiento de registro de inicio seguro

a) Autenticar usuarios autorizados, de acuerdo a la política de control de acceso de la institución, que deberá estar documentada, definida y socializada (*).

b) Llevar un registro de definición para el uso de privilegios especiales del sistema (*).

c) Llevar un proceso de monitoreo y registro de los intentos exitosos y fallidos de autenticación del sistema, registros de alarmas cuando se violan las políticas de seguridad del sistema (*).

d) Utilizar mecanismos como: uso de dominios de autenticación, servidores de control de acceso y directorios (*).

e) Restringir el tiempo de conexión de los usuarios, considerando las necesidades de la institución (*).

f) Controlar que no se muestren identificadores de aplicación ni de sistema, hasta que el proceso de registro de inicio se haya completado exitosamente (*).

g) Evitar que se desplieguen mensajes de ayuda durante el procedimiento de registro de inicio de sesión.

h) Validar la información de registro de inicio únicamente al terminar todos los datos de entrada, y en el caso que se presentara un error o se generara sentencias de error, el sistema no indique qué parte de los datos es correcta o incorrecta o emita mensajes propios de las características del sistema.

i) Limitar la cantidad de intentos permitidos de registro de inicio de sesión; por ejemplo, tres intentos (*).

j) Limitar el tiempo de dilación antes de permitir o rechazar más intentos adicionales del registro de inicio sin autorización específica (*).

7.17. Identificación y autenticación de usuarios

a) Rastrear utilizando los identificadores de usuario y evidenciar las actividades de las personas responsables de administraciones críticas de la institución (*).

b) Usar como excepción, y solo por temas de necesidad de la institución, identificadores de usuarios para un grupo de usuarios o de trabajo específico, el cual debe estar definido y documentado (*).

c) Las actividades de usuarios regulares no deben ser realizadas desde cuentas privilegiadas.

d) Evitar el uso de usuarios genéricos (*).

e) Utilizar métodos alternos a la contraseña, como los medios criptográficos, las tarjetas inteligentes, tokens o medios biométricos de autenticación (*).

f) La identificación de usuario es única e intransferible, por lo que, debe estar registrado y evidenciado en la política de acceso que no se permite el uso de una identificación de usuario de otra persona, y el responsable de toda actividad realizada con este identificador responderá a cualquier acción realizada con éste.

7.18. Sistema de gestión de contraseñas

a) Evidenciar en la política de accesos, la responsabilidad del buen uso de la contraseña y que debe ser secreta e intransferible (*).

b) Controlar el cambio de contraseña de los usuarios y del personal de tecnología y de los administradores de tecnología, en rangos de tiempo y complejidad (*).

c) Forzar el cambio de contraseña en el primer registro de acceso o inicio de sesión (*).

d) Generar un procedimiento formal para la administración y custodia de las contraseñas de acceso de administración e información crítica de la institución.

e) Documentar el control de acceso para los usuarios temporales.

f) Almacenar y transmitir las contraseñas en formatos protegidos (encriptados o codificados).

7.19. Uso de las utilidades del sistema

a) Restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles de un sistema en base a las siguientes directrices:

- uso de procedimientos de identificación, autenticación y autorización para programas utilitarios;
- separación de los programas utilitarios del software de aplicaciones;
- limitación del uso de programas utilitarios a la cantidad mínima viable de usuarios de confianza autorizados;
- autorización del uso de programas utilitarios no estándares de la entidad;
- limitación del tiempo de uso de programa utilitarios;
- registro de todo uso de programas utilitarios;
- retiro o inhabilitación de todos los programas utilitarios innecesarios;

7.20. Tiempo de inactividad de la sesión

a) Suspender las sesiones inactivas después de un período definido de inactividad sin consideración de lugar dispositivo de acceso

b) Parametrizar el tiempo de inactividad en los sistemas de procesamiento de información para suspender y cerrar sesiones

7.21. Limitación del tiempo de conexión

a) Utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo. Los siguientes son algunos ejemplos de estas restricciones:

b) Configurar espacios de tiempo predeterminados para procesos especiales (por ejemplo, transmisiones de datos o archivos, obtención de respaldos, mantenimientos programados, entre otros.)

c) Restringir los tiempos de conexión a las horas normales de oficina, si no se requiere tiempo extra u operaciones de horario prolongado;

d) Requerir la autenticación a intervalos determinados cuando lo amerite

e) Proporcionar accesos temporales para ciertas operaciones (por ejemplo, mediante tickets o tokens electrónicos temporales)

7.22. Control de acceso a las aplicaciones y a la información

a) Controlar el acceso de usuarios a la información y a las funciones del sistema de aplicación, de acuerdo con una política definida de control de acceso;

b) Suministrar protección contra acceso no autorizado por un programa utilitario, software del sistema operativo, software malicioso o cualquier otro software que pueda anular o desviar los controles de seguridad del sistema;

c) Evitar poner en riesgo otros sistemas con los que se comparten los recursos de información.

7.23. Restricción de acceso a la información

a) Controlar el acceso a las funciones de los sistemas y aplicaciones.

b) Definir mecanismos de control para los derechos de acceso de los usuarios, para lectura, escritura, eliminación y ejecución de información.

c) Definir y documentar mecanismos de control para los derechos de acceso de otras aplicaciones.

d) Generar mecanismos a fin de garantizar que los datos de salida de los sistemas de aplicación que manejan información sensible sólo contengan la información pertinente y que se envíe únicamente a terminales o sitios autorizados.

e) Generar revisiones periódicas de las salidas de los sistemas de aplicación para garantizar el retiro de la información redundante.

7.24. Aislamiento de sistemas sensibles

a) Identificar y documentar los sistemas sensibles y al responsable de la aplicación.

b) Identificar y registrar los riesgos, cuando una aplicación se ejecuta en un entorno compartido.

c) Identificar y registrar aplicaciones sensibles que se encuentra compartiendo recursos.

d) Las aplicaciones sensibles, por su criticidad para la institución, deberán ejecutarse en un computador dedicado, únicamente compartir recursos con sistemas de aplicación confiables, o utilizar métodos físicos o lógicos de aislamiento.

7.25. Computación y comunicaciones móviles

a) Evitar exposición de equipos portátiles en sitios inseguros, públicos y de alto riesgo. (*)

b) La información sensible, de alta criticidad o confidencial, debe estar en una partición específica del disco del equipo portátil, y resguardada bajo métodos de cifrado.

c) En la política para uso de equipos portátiles y comunicaciones móviles de la institución, deberá definir rangos de tiempo máximo que el equipo puede permanecer sin conexión a la red de la institución, a fin de que este actualice el antivirus y las políticas aplicadas por la institución.

d) En el proceso de respaldos de la institución, debe estar considerado específicamente los documentos definidos como críticos, sensibles o confidenciales de las diferentes áreas; además, en el proceso de respaldo del equipo portátil deberá definirse el responsable y procedimiento de acceso a esta información.

e) Dentro de la institución el equipo portátil deberá estar asegurado con medios físicos, mediante el uso de candados.

f) El personal que utiliza computadores portátiles y equipos móviles, deberá estar alerta de los riesgos adicionales que se originan y los controles que se deberán implementar.

7.26. Trabajo remoto

a) Las instituciones podrán autorizar la modalidad de trabajo remoto en circunstancias específicas, siempre que en la institución se apliquen las disposiciones de seguridad y los controles establecidos, cumpliendo con la política de seguridad de la información.

b) El funcionario deberá observar la seguridad física de la edificación y del entorno local existente en el sitio de trabajo remoto.

c) Deberá evitarse la conexión a redes inalámbricas que no posean la seguridad de acceso y autenticación adecuadas.

d) No se permite el uso de equipo de propiedad privada que no esté bajo el control y monitoreo de la institución (*).

e) Deberá definirse el trabajo que se permite realizar, las horas laborables, la confidencialidad de la información que se conserva y los sistemas y servicios internos para los cuales el trabajador tiene acceso autorizado.

f) Deberá considerarse la protección de antivirus y reglas del Firewall (*).

g) Deberán estar documentadas las reglas y directrices sobre el acceso de familiares y visitantes al equipo y a la información.

h) La institución deberá observar la disposición de una póliza de seguros para estos equipos.

i) Determinar procesos de monitoreo y auditoría de la seguridad del trabajo remoto que se realice.

j) Permitir al personal realizar trabajo remoto empleando tecnologías de comunicaciones cuando requiere hacerlo desde un lugar fijo fuera de su institución.

8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

8.1. Análisis y especificaciones de los requerimientos de seguridad

a) Definir los requerimientos de seguridad. Por ejemplo: criptografía, control de sesiones, etc. (*).

b) Definir los controles apropiados, tanto automatizados como manuales. En esta definición deben participar personal del requerimiento funcional y personal técnico que trabajarán en el sistema. Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas por falla o falta de seguridad. (*).

c) Si se adquieren productos, los contratos con el proveedor deben contemplar los requisitos de la seguridad identificados.

d) Cuando se proporciona funcionalidad adicional y ello causa un riesgo de la seguridad, tal funcionalidad se debe inhabilitar o cambiar. Información adicional sobre los criterios para los productos de la seguridad de la tecnología de la información se puede encontrar en la norma ISO/IEC15408 o en otras normas sobre evaluación y certificación, según sea el caso. La norma ISO/IEC TR 13335-3 proporciona directrices sobre el uso de procesos de gestión de riesgos para identificar los requisitos de los controles de la seguridad.

8.2. Validación de datos de entrada

a) Especificar y utilizar controles que aseguren la validez de los datos ingresados, en el punto de entrada de los mismos, controlando también parámetros de los sistemas (ej., %IVA, dirección IP del servidor).

b) Verificar los datos de entrada con controles que permitan la negación de ingreso de datos: duales, valores fuera de rango, caracteres no válidos, datos incompletos o ausentes, datos de controles inconsistentes o no autorizados, la secuencia de los datos, formatos incorrectos, inyección de código, etc.

c) Definir el estándar de respuesta ante errores de validación.

d) Definir convalidaciones para probar la credibilidad de los datos de entrada.

e) Crear un registro de las actividades implicadas en el proceso de entrada de datos.

8.3. Control de procesamiento interno

a) Incorporar controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores.

b) Utilizar controles de sesión en los sistemas.

c) Utilizar funciones de agregar, modificar y borrar para implementar los cambios en los datos. El borrado a través de los sistemas será siempre un borrado lógico de los datos.

d) Crear registros de auditoría, al insertar y actualizar datos; y, si se requiere según el sistema, se mantendrá el registro (logs) de consultas de datos.

e) Incorporar en los sistemas, validaciones necesarias para prevenir la ejecución de programas fuera de secuencia, en orden erróneo o de ejecución después de una falla.

f) Crear el procedimiento y/o herramientas para la revisión periódica de los registros de auditoría para detectar cualquier anomalía en la ejecución de las transacciones.

g) Identificar, crear y utilizar programas para la recuperación de datos después de fallas, con el fin de garantizar el procesamiento correcto de los datos.

h) Utilizar controles para mantener integridad de registros y archivos.

i) Utilizar controles para protección contra ataques por desbordamiento/exceso en el buffer.

j) Definir y ejecutar periódicamente, procedimientos de recuperación de sistemas, que verifiquen la ejecución de los sistemas en caso de una falla o desastre, esto estará a cargo del administrador técnico de la aplicación o sistema.

k) Definir los procedimientos que aseguren el orden correcto de ejecución de los sistemas, la finalización programada en caso de falla y la detención de las actividades de procesamiento, hasta que el problema sea resuelto.

8.4. Integridad del mensaje

a) Cuando una aplicación tenga previsto el envío de mensajes que contengan información reservada o confidencial, se implementarán los controles criptográficos determinados en el punto "8.6 Política sobre uso de controles criptográficos".

8.5. Validación de datos de salidas

a) Incorporar el control de conciliación de datos, para asegurar el procesamiento de todos los datos.

b) Suministrar información para que el lector o sistema de procesamiento subsiguiente determine la exactitud, totalidad, precisión y clasificación de la información.

c) Desarrollar procedimientos para responder a las pruebas de validación de salidas.

d) Crear un registro de las actividades del proceso de validación de la salida de datos.

e) Generar protocolos de pruebas y los casos de pruebas para la validación de los datos de salida.

8.6. Política sobre el uso de controles criptográficos.

a) Identificar el nivel requerido de protección de datos que se almacenará en el sistema, considerando: el tipo, fortaleza y calidad del algoritmo de cifrado (encriptación) requerido.

b) Utilizar controles criptográficos para la protección de claves de acceso a sistemas, datos y servicios. Las claves deberán ser almacenadas de manera codificada, cifrada (encriptada) en la base de datos y/o en archivos de parámetros.

c) Desarrollar procedimientos de administración de claves, de recuperación de información cifrada en caso de pérdida, de compromiso o daño de las claves y de reemplazo de claves de cifrado.

d) Utilizar controles de cifrado (criptográficos) para la transmisión de información clasificada, fuera del ámbito de la institución.

e) Utilizar controles de cifrado (criptográficos) para la protección de la información sensible transportada por medios móviles o removibles, por dispositivos especiales, o a través de los medios de comunicación.

f) Definir las normas de controles de cifrado (criptográficos) que se adoptarán, para la implementación eficaz en toda la institución, estableciendo la solución a usar para cada proceso del negocio.

g) Los responsables del área de Tecnologías de la Información propondrán la siguiente asignación de funciones:

- Implementación de la Política de Controles
- Administración de claves: gestión de claves, incluyendo su generación

h) Se debe garantizar:

- Confidencialidad: uso de cifrado (encriptación) de la información para proteger información sensible o crítica, bien sea almacenada o transmitida
- Integridad / autenticidad: uso de firmas electrónicas o códigos de autenticación de mensajes para proteger la autenticidad e integridad de información sensible o crítica transmitida o almacenada
- No-repudio: uso de técnicas de cifrado (criptográficas) para obtener prueba de la ocurrencia o no ocurrencia de un evento o acción.

i) Definir los algoritmos de cifrado (encriptación) que se utilizarán en toda la institución, dependiendo del tipo de control a aplicar, el propósito y el proceso del negocio. Esta definición debe ser periódicamente revisada y actualizada.

j) Uso de firma electrónica:

- Utilizar certificados electrónicos de Entidad de Certificación de Información reconocidas por el Estado Ecuatoriano para la firma de cualquier tipo de documento, mensaje de dato, transacción que se proceso electrónicamente o para comunicaciones entre sistemas, aplicaciones y medios físicos.
- Utilizar los certificados electrónicos emitidos bajo estándares por las Entidades de Certificación de Información, las cuales deben ser instituciones u organizaciones reconocidas, con controles y procedimientos idóneos establecidos para proporcionar el grado requerido de confianza.
- Uso de los certificados electrónicos según el ámbito para la cual fue generado.

8.7. Gestión de claves

a) Protección de claves cifradas (criptográficas):

- Implementar un sistema de administración de claves cifradas (criptográficas) para respaldar la utilización por parte de la institución, de los dos tipos de técnicas criptográficas: técnicas de clave secreta (criptografía simétrica) y técnicas de clave pública (criptografía asimétrica).
- Proteger todas las claves contra modificación y destrucción, y las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada.
- Proporcionar una protección adecuada al equipamiento utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.
- Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.
- Habilitar en los sistemas, la generación de claves en la creación de usuarios. Se generará la primera clave la cual deberá obligatoriamente cambiar el propio usuario la primera vez que ingresa al sistema.
- Generar y obtener certificados de claves públicas.
- Distribuir la primera clave a los usuarios, incluyendo la forma de activar y confirmar la recepción de la clave. Luego, a través de un correo electrónico recibirá un acceso al sistema, el cual validará la entrega de la clave y la obligatoriedad de cambiar dicha clave.
- Almacenar las claves cifradas (encriptadas).
- Incorporar funcionalidad para cambiar o actualizar las claves, incluyendo reglas sobre cuándo cambiarlas, cómo hacerlo y la forma en que los usuarios autorizados tendrán acceso a ellas.
- Incorporar funcionalidad para tratar las claves perdidas. Bajo pedido del usuario que pierde una clave se generará una nueva, la entrega será a través del procedimiento definido para la entrega de la primera clave.
- Permitir revocar las claves, incluyendo la forma de retirarlas o desactivarlas cuando las claves se han puesto en peligro o cuando un usuario se retira de la institución.
- Incorporar funcionalidad para recuperar claves perdidas o corruptas como parte de la gestión de continuidad de los servicios informáticos.
- Permitir archivar claves para información archivada o con copia de respaldo.
- Permitir la destrucción de claves que se dejen de utilizar.
- Registrar y auditar las actividades relacionadas con la gestión de claves.

b) Normas, Procedimientos y Métodos:

- Redactar las normas y procedimientos necesarios para generar claves para diferentes sistemas criptográficos y diferentes aplicaciones, incluyendo fechas de inicio y caducidad de vigencia de las claves.

- Redactar las normas y procedimientos necesarios para generar y obtener certificados de clave pública de manera segura.
- Redactar las normas y procedimientos para distribuir las claves de forma segura a los usuarios, incluyendo información sobre cómo deben activarse cuándo se reciben las mismas.
- Redactar las normas y procedimientos para almacenar claves, incluyendo la forma de acceso a las mismas, por parte de los usuarios autorizados.
- Redactar las normas y procedimientos para cambiar o actualizar claves, incluyendo reglas sobre cuándo y cómo deben cambiarse las claves.
- Redactar las normas y procedimientos para revocar claves, incluyendo cómo deben retirarse o desactivarse las mismas.
- Redactar las normas y procedimientos para archivar claves, por ejemplo, para la información archivada o resguardada.
- Redactar las normas y procedimientos para destruir claves.
- Redactar las normas y procedimientos para registrar y auditar las actividades relativas a la administración de claves.

8.8. Control del software operativo

a) Definir y aplicar procesos de control de cambios para la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.

b) Definir el proceso de paso a producción para cada sistema.

c) Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.

d) Asignar un responsable de la implantación de cambios por sistema (no podrá ser personal que pertenezca al área de desarrollo o mantenimiento), quien tendrá como funciones principales:

- Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.
- Asegurar que los aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.
- Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable, del área encargada del testeo y del usuario final.
- Rechazar la implementación en caso de encontrar defectos

e) Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones para el paso a producción, el informe de pruebas previas y el informe de paso a producción.

f) Disponer del informe de paso a producción, el cual contendrá información de todos los cambios a realizar y el plan de contingencia.

g) Guardar o instalar únicamente los ejecutables y cualquier elemento necesario para la ejecución de un software en el ambiente de producción.

h) Implementar el ensayo en el ambiente de pruebas. Este ambiente debe ser similar al ambiente de producción. El ensayo será en base al informe de paso a producción. Se ejecutarán todas las acciones definidas y se realizarán pruebas sobre capacidad de uso, seguridad, efectos en otros sistemas y facilidad para el usuario.

i) Llevar un registro de auditoría de las actualizaciones realizadas.

j) Retener las versiones previas del sistema, como medida de contingencia.

k) Denegar permisos de modificación a los desarrolladores, sobre los programas fuentes bajo su custodia.

l) Usar un sistema de control de configuración para mantener el control del software instalado, así como de la documentación del sistema.

m) Entregar acceso físico o lógico al ambiente producción únicamente para propósitos de soporte, cuando sea necesario y con aprobación del responsable del área de Tecnologías de la Información, esto se realizará tanto para usuarios internos de la dirección como para proveedores.

n) Monitorear las actividades de soporte realizadas sobre el ambiente de producción.

8.9. Protección de los datos de prueba del sistema

a) Identificar por cada sistema, los datos que pueden ser copiados de un ambiente de producción a un ambiente de pruebas.

b) Efectuar pruebas de los sistemas en el ambiente de pruebas, sobre datos extraídos del ambiente de producción.

c) Solicitar autorización formal para realizar una copia de la base de datos de producción como base de datos de prueba.

d) Personalizar los datos en el ambiente de pruebas, eliminando las contraseñas de producción y generando nuevas para pruebas.

e) Identificar los datos críticos que deberán ser modificados o eliminados del ambiente de pruebas.

f) Aplicar los mismos procedimientos de control de acceso que existen en la base de producción.

g) Eliminar inmediatamente, una vez completadas las pruebas, la información de producción utilizada.

h) Registrar la copia y la utilización de la información para futuras auditorías.

i) Controlar que la modificación, actualización o eliminación de los datos operativos (de producción) serán realizados a través de los sistemas que procesan esos datos, y de acuerdo al esquema de control de accesos implementado en los mismos.

j) Se considerarán como excepciones, los casos en que se requiera realizar modificaciones directamente sobre la base de datos. El Oficial de Seguridad de la Información definirá los procedimientos para la gestión de dichas excepciones que contemplarán lo siguiente:

- Se generará una solicitud formal para la realización de la modificación o actualización del dato. No se aceptará eliminación de datos bajo ninguna circunstancia.

- El Propietario de la Información afectada y el Oficial de Seguridad de la Información aprobarán la ejecución del cambio evaluando las razones por las cuales se solicita.

- Se generarán cuentas de usuario de emergencia para ser utilizadas en la ejecución de excepciones. Las mismas serán protegidas mediante contraseñas, la cuales estarán sujetas al procedimiento de administración de contraseñas críticas y habilitadas sólo ante un requerimiento de emergencia y por el lapso que ésta dure.

- Se designará un encargado de implementar los cambios, el cual no será personal del área de Desarrollo. En el caso de que esta función no pueda ser separada del área de Desarrollo, se aplicarán controles adicionales de acuerdo a la separación de funciones.

- Se registrarán todas las actividades realizadas con las cuentas de emergencia. Dicho registro será revisado posteriormente por el Oficial de Seguridad.

8.10. Control de acceso al código fuente de los programas

a) Asignar a un Administrador de programas fuentes, quien tendrá en custodia los programas fuentes y deberá:

- Utilizar un manejador de versiones para los código fuentes, proporcionar permisos de acceso a los desarrolladores bajo autorizaciones.

- Proveer al área de Desarrollo los programas fuentes solicitados para su modificación, manteniendo en todo momento la correlación programa fuente/ejecutable.

- Llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, programador, autorizador, versión, fecha de última modificación y fecha/hora de compilación y estado (en modificación o en producción).

- Verificar que el autorizador de la solicitud de un programa fuente sea el designado para la aplicación, rechazando el pedido en caso contrario.

- Registrar cada solicitud aprobada.

- Administrar las distintas versiones de una aplicación.

- Asegurar que un mismo programa fuente no sea modificado simultáneamente por más de un desarrollador, sin un manejador de versiones.

b) Establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen.

c) Establecer que el responsable de implantación en producción efectuará la generación del programa objeto o ejecutable que estará en producción (compilación), a fin de garantizar tal correspondencia.

d) Desarrollar un procedimiento que garantice que cuando se migre a producción el módulo fuente, de preferencia se cree el código ejecutable correspondiente de forma automática de preferencia.

e) Evitar que la función de Administrador de programas fuentes, sea ejercida por personal que pertenezca al área de desarrollo y/o mantenimiento.

f) Prohibir la guarda de programas fuentes históricos (que no sean los correspondientes a los programas operativos) en el ambiente de producción.

g) Prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permiten la generación y/o manipulación de los programas fuentes.

h) Realizar las copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos como respaldos de información.

i) Cuando sea posible, las bibliotecas fuente de programas no se deberán mantener en los sistemas operativos.

j) El código fuente de programas y las bibliotecas fuente de programas se deberán gestionar de acuerdo con los procedimientos establecidos.

k) El personal de soporte no debe tener acceso al código fuente de programas.

l) La actualización del código fuente de programas y de los elementos asociados, así como la emisión de fuentes de programa a los programadores, solamente se deberá efectuar después de recibir la autorización apropiada.

m) Conservar un registro para auditoría de todos los accesos al código fuente de programas.

n) El mantenimiento y el copiado del código fuente de programas deberán estar sujetos a un procedimiento estricto de control de cambios.

8.11. Procedimiento de control de cambios

a) Verificar que los cambios sean propuestos por usuarios autorizados y se respete los términos y condiciones que surjan de la licencia de uso, en caso de existir.

b) Elaborar el informe de paso de pruebas a producción, que deberá contener el detalle de los cambios y acciones a ejecutar, tanto de software, bases de datos y hardware:

- Archivos a modificar;
- Script de base de datos a ejecutar en la secuencia correcta de ejecución;
- Script de inicialización de datos;
- Creación de directorios;
- Script de creación de tareas periódicas, en caso de ser necesario;
- Plan de contingencia;
- Protocolo de pruebas de verificación el cambio;
- Definir el punto de no retorno;
- Definir las condiciones para determinar la restauración al estado anterior.

c) Obtener aprobación formal por parte del responsable del área de Tecnologías de la Información para las tareas detalladas, antes de comenzar las tareas.

d) Mantener un registro de los niveles de autorización acordados.

e) Implementar funcionalidades para que se pueda solicitar la autorización del propietario de la información (ej., información personal), cuando se hagan cambios a sistemas de procesamiento de la misma.

f) Notificar a los usuarios del sistema sobre el cambio a realizar. Se enviará una notificación para informar sobre el tiempo que durará la ejecución del cambio y para informar cuando se haya terminado la ejecución del cambio.

g) Abrir ventanas de mantenimiento con una duración definida, en la cual se contemple las acciones del cambio, pruebas y configuraciones.

h) Revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios.

i) Solicitar la revisión del Oficial de Seguridad de la Información para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.

j) Efectuar las actividades relativas al cambio en el ambiente de pruebas.

k) Obtener la aprobación por parte del usuario autorizado y del área de pruebas mediante pruebas en el ambiente correspondiente.

l) Actualizar la documentación para cada cambio implementado, tanto en los manuales de usuario como en la documentación operativa.

m) Mantener un control de versiones para todas las actualizaciones de software.

n) Garantizar que la implementación se llevará a cabo minimizando la discontinuidad de las actividades y sin alterar los procesos involucrados.

o) Definir si los cambios a realizar tienen impacto sobre la continuidad del servicio. Si un cambio implica mucha funcionalidad o impacto al software base o infraestructura, se deberá realizar un procedimiento más complejo de cambio, para que se apruebe con un plan de contingencia y se identifiquen los riesgos posibles.

8.12. Revisión técnica de las aplicaciones después de los cambios en el sistema operativo

a) Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.

b) Garantizar que los cambios en el sistema operativo sean informados con anterioridad a la implementación.

c) Probar que los cambios realizados retornen la funcionalidad esperada.

d) Realizar las pruebas inmediatamente después de realizar el cambio y durante la ventana de mantenimiento definida para el cambio.

e) Disponer de un protocolo de pruebas a realizar.

f) Entregar un informe de las pruebas realizadas.

g) Identificar si existen problemas con los cambios, para aplicar el plan de contingencia o realizar el retorno al estado anterior al cambio.

8.13. Restricción del cambio de paquetes de software

a) Disponer de la autorización del Responsable del área de Tecnologías de la Información que apruebe el cambio.

b) Analizar los términos y condiciones de la licencia, si es del caso, a fin de determinar si las modificaciones se encuentran autorizadas.

c) Determinar la conveniencia de que la modificación sea efectuada por la institución, por el proveedor o por un tercero, y evaluar el impacto.

d) Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

e) Conservar el software original que se va ha cambiar y los cambios se deberán aplicar a una copia claramente identificada.

f) Definir un proceso de gestión de las actualizaciones del software para asegurarse de que los parches más actualizados aprobados y las actualizaciones de las aplicaciones están instalados en todo el software autorizado.

g) Probar y documentar en su totalidad todos los cambios, de manera que se puedan volver a aplicar, si es necesario, para mejoras futuras del software.

8.14. Fuga de información

a) Explorar los medios y comunicaciones de salida para determinar la información oculta.

b) Garantizar que un tercero no pueda deducir, extraer información de las comunicaciones, sistemas de modulación o de almacenamiento, a partir de un comportamiento específico.

c) Adquirir o desarrollar programas acreditados o productos ya evaluados.

d) Realizar un monitoreo regular de las actividades del personal y del sistema.

e) Realizar un monitoreo del uso de los recursos en los sistemas de computador y transmisión de datos por la red.

f) Restringir el envío de información a correos externos no institucionales.

g) Prevenir y restringir el acceso no autorizado a la red.

h) Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.

i) Controlar el acceso y las modificaciones al código instalado.

j) Utilizar herramientas para la protección contra la infección del software con código malicioso.

8.15. Desarrollo de software contratado externamente

a) Definir acuerdos de licencias, acuerdos de uso, propiedad de código y derechos conferidos.

b) Definir los requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.

c) Definir procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.

d) Verificar el cumplimiento de las condiciones de seguridad requeridas.

e) Definir acuerdos de custodia de los fuentes del software o convenios de fideicomiso (y cualquier otra información requerida) en caso de quiebra de la tercera parte.

f) Realizar pruebas antes de la instalación para detectar códigos troyanos o maliciosos.

8.16. Control de las vulnerabilidades técnicas

a) Disponer de un inventario completo y actual de los activos de software. El inventario servirá para dar soporte a la gestión de la vulnerabilidad técnica e incluye los siguientes datos: vendedor

del software, números de versión, estado actual de despliegue y las personas de la institución responsables del software.

b) Definir e instaurar las funciones y responsabilidades asociadas con la gestión de la vulnerabilidad técnica, incluyendo el monitoreo de la vulnerabilidad, la evaluación de riesgos de la vulnerabilidad, el uso de parches, el rastreo de activos y todas las responsabilidades de coordinación requeridas.

c) Identificar los recursos de información que se van a utilizar para identificar las vulnerabilidades técnicas pertinentes y para mantener la concienciación sobre ellas para el software y otras tecnologías, con base en la lista de inventario de activos.

d) Actualizar los recursos de información en función de los cambios en el inventario o cuando se encuentren recursos nuevos o útiles.

e) Definir una línea de tiempo para reaccionar ante la notificación de vulnerabilidades técnicas potenciales pertinentes.

f) Identificar los riesgos asociados a una vulnerabilidad potencial y las acciones que se han de tomar; tales acciones podrían involucrar el uso de parches en los sistemas vulnerables y/o la aplicación de otros controles.

g) Definir la urgencia y las acciones a tomar para tratar la vulnerabilidad técnica identificada, se realizará conforme a los controles relacionados con la gestión de cambios o siguiendo los procedimientos de respuesta ante incidentes de seguridad de la información.

h) Evaluar los riesgos asociados con la instalación de un parche para cubrir vulnerabilidades. Los riesgos impuestos por la vulnerabilidad se deberán comparar con los riesgos de instalar el parche.

i) Probar y evaluar los parches antes de su instalación para garantizar que son eficaces y no producen efectos secundarios intolerables. Estas pruebas se realizarán en un ambiente similar al de producción.

j) Apagar los servicios o capacidades relacionadas con la vulnerabilidad.

k) Adaptar o agregar controles de acceso; por ejemplo, cortafuegos (firewalls), en las fronteras de la red.

l) Aumentar el monitoreo para detectar o prevenir los ataques reales.

m) Crear conciencia en los desarrolladores sobre la vulnerabilidad.

n) Conservar un registro para auditoría de todos los procedimientos efectuados.

o) Monitorear y evaluar a intervalos regulares las vulnerabilidades técnicas, para garantizar eficacia y eficiencia.

p) Tratar primero los sistemas con alto riesgo.

9. GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

9.1. Reporte sobre los eventos de seguridad de la información

a) Instaurar un procedimiento formal para el reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidente, que establezca la acción que se ha de tomar al recibir el reporte sobre un evento que amenace la seguridad de la información (*).

b) Establecer un punto de contacto (Oficial de Seguridad de la Información) para el reporte de los eventos de seguridad de la información. Es conveniente garantizar que este punto de contacto sea conocido en toda la institución, siempre esté disponible y pueda suministrar respuesta oportuna y adecuada. Todos los empleados, contratistas y usuarios contratados por los proveedores deberán tomar conciencia de su responsabilidad para reportar todos los eventos de seguridad de la información lo más pronto posible.

c) Cuando un incidente se produzca, el funcionario en turno responsable del equipo o sistema afectado, debe realizar las siguientes acciones en su orden (*):

- Identificar el incidente
- Registrar el incidente en una bitácora de incidentes (reporte de eventos) incluyendo fecha, hora, nombres y apellidos del funcionario en turno, departamento o área afectada, equipo o sistema afectado y breve descripción del incidente.
- Notificar al Oficial de Seguridad de la Información de la institución.
- Clasificar el incidente de acuerdo al tipo de servicio afectado y al nivel de severidad.
- Asignar una prioridad de atención al incidente en el caso de que se produjeran varios en forma simultánea.
- Realizar un diagnóstico inicial, determinando mensajes de error producidos, identificando los eventos ejecutados antes de que el incidente ocurra, recreando el incidente para identificar sus posibles causas.

- Escalar el incidente en el caso que el funcionario en turno no pueda solucionarlo, el escalamiento deberá ser registrado en la bitácora de escalamiento de incidentes. El funcionario en turno debe escalar el incidente a su jefe inmediato, en el caso en el que el funcionario no tuviere un jefe al cual escalarlo, este debe solicitar soporte al proveedor del equipo o sistema afectado.

- Investigar y diagnosticar en forma definitiva las causas por las cuales se produjo el incidente.

- Resolver y restaurar el servicio afectado por el incidente debido a la para de un equipo o un sistema, incluyendo un registro de la solución empleada en la bitácora de incidentes.

- Cerrar el incidente, actualizando el estado del registro del incidente en la bitácora de incidentes a "Resuelto". Confirmar con el funcionario en turno, responsable del equipo o del sistema de que el incidente ha sido resuelto.

9.2. Reporte sobre las debilidades en la seguridad

a) Todos los empleados, contratistas y usuarios de tercera partes deberán informar sobre estos asuntos a su director o directamente a su proveedor de servicio, tan pronto sea posible para evitar los incidentes de seguridad de la información. Los mecanismos de reporte deberán ser fáciles, accesibles y disponibles. Se les debe informar a ellos que, en ninguna circunstancia, deberán intentar probar una debilidad sospechada.

b) Cuando un empleado, contratista o usuario contratado por un proveedor detecte una vulnerabilidad o debilidad en un equipo, sistema o servicio deberá ejecutar las siguientes acciones:

- Notificar a su jefe inmediato y este al Oficial de Seguridad de la Información de la debilidad o vulnerabilidad detectada.

- Registrar la fecha, hora, apellidos y nombres del funcionario que detectó la debilidad o vulnerabilidad, descripción de la debilidad, descripción de posibles incidentes de seguridad que pudieran ocurrir producto de esta debilidad. El responsable de llevar este reporte denominado "Reporte de vulnerabilidades o debilidades de la seguridad de la información" es el Oficial de Seguridad de la Información.

- Nunca, por razón alguna, deberá intentar probar la debilidad o vulnerabilidad detectada en la seguridad. El ensayo de las vulnerabilidades se podría interpretar como un posible uso inadecuado del sistema, equipo o servicio y también podría causar daño al sistema o servicio de información y eventualmente podría recaer en una responsabilidad legal.

- El Oficial de Seguridad de la Información deberá tomar las medidas pertinentes para prevenir o eliminar la vulnerabilidad o debilidad detectada.

9.3. Responsabilidades y procedimientos

a) Además de la bitácora de registro de incidentes y el reporte de vulnerabilidades de la seguridad de la información, el monitoreo de los sistemas, las alertas y las vulnerabilidades, se deberán establecer y ejecutar un procedimiento para la gestión de incidentes.

b) Identificar y clasificar los diferentes tipos de incidentes de seguridad de la información.

c) Identificar y analizar las posibles causas de un incidente producido.

d) Planificar e implementar acciones correctivas para evitar la recurrencia del incidente

e) Notificar a todos los funcionarios afectados por el incidente de la restauración del equipo, sistema o servicio afectado, una vez esté solucionado el incidente.

f) El Oficial de Seguridad de la Información, emitirá un reporte a los jefes de las áreas afectadas por el incidente.

g) Recolectar y asegurar pistas de auditoría y toda la evidencia relacionada con el incidente.

9.4. Aprendizaje debido a los incidentes de seguridad de la información

a) La información que se obtiene de la evaluación de los incidentes de seguridad de la información se debe utilizar para identificar los incidentes recurrentes o de alto impacto.

b) Determinar el número de incidentes por tipo, el número de incidentes graves, el tiempo medio de resolución de incidentes.

c) Determinar el costo promedio por incidente.

d) Determinar el número de incidentes recurrentes.

e) Determinar la frecuencia de un incidente recurrente.

9.5. Recolección de evidencias

a) Desarrollar y cumplir procedimientos internos cuando se recolecta y se presenta evidencia con propósitos de acción disciplinaria dentro de la institución.

b) Asegurar que los sistemas de información cumplan con las normas legales para la producción de evidencia, para lograr la admisibilidad, calidad y cabalidad de la misma.

c) Para lograr el peso de la evidencia, se debe demostrar la calidad y cabalidad de los controles empleados para proteger correcta y consistentemente la evidencia (es decir, evidencia del control del proceso) en todo el periodo en el cual la evidencia por recuperar se almacenó y procesó, mediante un rastreo sólido de la evidencia. En general, dicho rastreo sólido se puede establecer en las siguientes condiciones:

- Se deberán tomar duplicados o copias de todos los medios removibles, la información en los discos duros o la memoria para garantizar la disponibilidad; es conveniente conservar el registro de todas las acciones durante el proceso de copiado y dicho proceso debería tener testigos; y, el medio y el registro originales se deberán conservar intactos y de forma segura;

- Se debe proteger la integridad de todo el material de evidencia. El proceso de copia del material de evidencia debe estar supervisado por personal de confianza y se debe registrar la información sobre cuándo y cómo se realizó dicho proceso, quién ejecutó las actividades de copiado y qué herramientas o programas se utilizaron.

10. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

10.1. Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio

a) El Responsable del área de Tecnologías de la Información o su similar será designado como coordinador de continuidad de los servicios informáticos, que se encargará de supervisar el proceso de elaboración e implantación del plan de continuidad, así como de la seguridad del personal.

b) Identificar los activos involucrados en los procesos críticos de los servicios informáticos, así como de las actividades que se deben realizar.

c) Elaborar la política de continuidad de los servicios informáticos determinando los objetivos y el alcance del plan, así como las funciones y responsabilidades; un documento que establezca a alto nivel los objetivos, el alcance y las responsabilidades en la gestión de la continuidad. Por ejemplo, la plantilla del documento debería contener:

- INTRODUCCIÓN: Detallando de forma resumida de que se trata, la estructura del documento y que se persigue.

- OBJETIVOS: que se satisfacen con la aplicación de la política, como se garantizará continuidad de las actividades y de los servicios, planes adicionales de contingencia.

- ALCANCE: Procesos y operaciones que son cubiertos y recursos que utilizan los procesos u operaciones

- RESPONSABILIDADES: Diferentes responsables implicados en la gestión de la continuidad de los servicios informáticos

d) Garantizar la continuidad incorporando los procesos generados en la estructura de la institución.

10.2. Continuidad del negocio y evaluación de riesgos

a) Definir los procesos y actividades de los servicios y aplicaciones,

b) Entender las complejidades e interrelaciones existentes entre equipamiento, personas, tareas, departamentos, mecanismos de comunicación y relaciones con proveedores externos, los cuales pueden prestar servicios críticos que deben ser considerados.

c) Identificar y valorar el impacto de las interrupciones de los procesos, aplicaciones y servicios de los servicios informáticos, para cuantificar y calificar los impactos y saber sus efectos.

d) Identificar el tiempo máximo de interrupción permitida para cada servicio o aplicación crítico, por ejemplo, 30 minutos, una hora o un día.

e) Analizar los riesgos, identificando las amenazas sobre los activos y su probabilidad de ocurrencia.

f) Analizar las vulnerabilidades asociadas a cada activo y el impacto que puedan provocar sobre la disponibilidad.

g) Obtener un mapa de riesgos que permita identificar y priorizar aquellos que pueden provocar una paralización de las actividades de la institución.

h) Crear una estrategia de gestión de control de riesgos y el plan de acción.

10.3. Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información

a) Definir los equipos para ejecución del plan, donde se destacan las funciones claves que serán realizadas por los responsables:

- Responsables de respuestas a incidentes: analizan el impacto del incidente;

- Logística: responsable de reunir todos los medios para ayudar a la puesta en operación de las actividades;
- Recuperación: puesta en servicio de la infraestructura.

b) Desarrollar los procedimientos indicando el objetivo y el alcance, considerando las actividades y los tiempos de recuperación.

c) Difundir y capacitar al personal responsable en los conceptos que contemplan la continuidad de los servicios informáticos.

d) Definir las Estrategias:

- Seleccionar los sitios alternos y de almacenamiento externo;
- Duplicado de los registros tanto físicos como electrónicos;
- Incorporar RAID en los discos de los servidores;
- Duplicar el suministro eléctrico;
- Estrategia de reinicio de las actividades;
- Contratos de mantenimiento preventivo y correctivo;
- Estrategia adecuada de respaldos;
- Seguros para los activos:
- Métodos, procedimientos y procesos para la recuperación de los servicios.

10.4. Estructura para la planificación de la continuidad del negocio

a) Mantener los documentos de los procesos actualizados, utilizando la Gestión de Cambios.

b) Crear planes de respuesta a los incidentes.

c) Definir los calendarios de pruebas e informes.

d) Definir los acuerdos de niveles de servicios internos y con proveedores.

e) Definir los contratos para servicios de recuperación, si fuera el caso.

f) Definir las condiciones para activar los planes que describen el proceso a seguir antes de activar cada plan, así como sus responsabilidades.

g) Describir los procedimientos de respaldo para desplazar las actividades esenciales de los servicios informáticos o los servicios de soporte a lugares temporales alternos, y para devolver la operatividad de los procesos en los plazos establecidos.

h) Describir los procedimientos de reanudación con las acciones a realizar para que las operaciones de los equipos y servicios vuelvan a la normalidad.

i) Definir los activos y recursos necesarios para ejecutar los procedimientos de emergencia, respaldo y reanudación de los servicios.

j) Distribuir la política, estrategias, procesos y planes generados.

10.5. Pruebas, mantenimiento y revisión de los planes de continuidad del negocio

a) Evaluar la capacidad de respuesta ante desastres verificando los tiempos de respuesta, validez de los procedimientos y capacidad de los responsables. Los resultados obtenidos permitirá actualizar y mantener los planes establecidos.

b) Realizar pruebas de:

- Validez: revisar y discutir el plan;
- Simulación: escenario que permitirá verificar el plan de continuidad;
- Actividades críticas: pruebas en un entorno controlado sin poner en peligro la operación de los servicios informáticos;
- Completa: interrupción real y aplicación del plan de continuidad.

c) Realizar auditorías tanto internas como externas, identificando el tipo y alcance de la auditoría a realizar, se entregará un plan de medidas correctivas para llevar a cabo las recomendaciones acordadas.

d) Ejecutar auto-evaluaciones del plan de continuidad, estrategias y procesos generados.

11. CUMPLIMIENTO

11.1. Identificación de la legislación aplicable

a) Inventariar todas las normas legales, estatutarias, reglamentarias y contractuales pertinentes para cada programa de software, servicio informático y en general todo activo de información que utiliza la institución.

b) Organizar para cada activo de información las normas legales, estatutarias, reglamentarias y contractuales pertinentes.

c) Considerar la normas y leyes más generales relacionadas a la gestión de los datos e información electrónica en el gobierno. A saber:

- Constitución de la República del Ecuador
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos
- Ley Orgánica de Transparencia y Acceso a la Información Pública
- Ley del Sistema Nacional de Registro de Datos Públicos
- Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva
- Ley Orgánica y Normas de Control de la Contraloría General del Estado
- Leyes y normas de control del sistema financiero
- Leyes y normas de control de empresas públicas
- Ley del Sistema Nacional de Archivos
- Decreto Ejecutivo No. 1014 sobre el uso de Software Libre en la Administración Pública
- Decreto Ejecutivo No. 1384 sobre Interoperabilidad Gubernamental en la Administración Pública
- Otras normas cuya materia trate sobre la gestión de los activos de información en las entidades de la Administración Pública

11.2. Derechos de Propiedad Intelectual

a) Adquirir software únicamente a proveedores reconocidos para garantizar que no se violen derechos de propiedad intelectual. Si el Software es Libre Opensource se considerará los términos de las licencias públicas generales.

b) Implementar mecanismos para concienciar sobre las políticas para proteger derechos de propiedad intelectual y las acciones disciplinarias para el personal que las viole. Se aplica tanto al software libre como al privativo.

c) Mantener registros apropiados de los activos de información para proteger los derechos de propiedad intelectual. Se aplica tanto al software libre como al privativo.

d) Custodiar evidencia de la propiedad de licencias o suscripciones, contratos, discos maestros, manuales y toda la información relevante del software que se utiliza.

e) Controlar y asegurar que no se exceda el número máximo de usuarios permitidos para un programa de software. Se aplica tanto al software libre como al privativo, donde corresponda.

f) Verificar que se instale únicamente software autorizado y con las respectivas licencias en el caso de utilizar software privativo.

g) Cumplir los términos y condiciones de uso para el software y la información, obtenidos de la Internet o proveedores (programas freeware, shareware, demostraciones o programas para pruebas).

h) Controlar que no se duplique, convierta en otro formato, ni extraiga contenidos de grabaciones de audio y video, si no está expresamente permitido por su autor o la persona que tenga los derechos sobre el material.

i) Controlar que no se copie total ni parcialmente software privativo, códigos fuente y la documentación de programas de software con derechos de propiedad intelectual. Se exceptúa los programas de software libre bajo los términos de sus licencias públicas.

j) Definir y aplicar una licencia pública general al software desarrollado por la institución o contratado a terceros como desarrollo, para proteger la propiedad intelectual.

k) Exigir a los funcionarios que utilicen solo software desarrollado, provisto o aprobado por la institución.

11.3. Protección de registros en cada entidad

a) Clasificar los registros electrónicos y físicos por tipos, especificando los periodos de retención y los medios de almacenamiento, como discos, cintas, entre otros.

b) Mantener la documentación y especificaciones técnicas de los algoritmos y programas utilizados para el cifrado y descifrado de archivos y toda la información relevante relacionada con claves, archivos criptográficos o firmas electrónicas, para permitir el descifrado de los registros durante el periodo de tiempo para el cual se retienen.

c) Establecer un procedimiento para revisar el nivel de deterioro de los medios utilizados para almacenar los registros. Los procedimientos de almacenamiento y manipulación se deberán implementar según las recomendaciones del fabricante. Para almacenamiento a largo plazo, se recomienda considerar el uso cintas y discos digitales utilizando formatos de archivos y datos abiertos.

d) Establecer un procedimiento para garantizar el acceso a los datos e información registrada, tanto el medio como el formato, durante todo el periodo de retención.

e) Establecer un procedimiento para cambiar o actualizar la tecnología del medio en el cual se almacenan los activos de información y registros

de acuerdo a las innovaciones tecnológicas disponibles en el mercado.

f) Los sistemas de almacenamiento de datos se deberán seleccionar de manera que los datos requeridos se puedan recuperar en el periodo de tiempo y en formatos legibles, dependiendo de los requisitos que se deben cumplir.

g) Garantizar la identificación de los registros y el periodo de retención de los mismos tal como se defina en normas legales ecuatorianas. Este sistema debe permitir la destrucción adecuada de los registros después de este periodo, si la entidad no los necesita y las normas así lo especifican.

h) Establecer y difundir en la entidad las directrices sobre retención, almacenamiento, manipulación y eliminación de registros e información.

i) Inventariar las fuentes de información clave.

j) Implementar controles apropiados para proteger los registros contra pérdida, destrucción y falsificación de la información. Utilizar como referencia para la gestión de los registros de la institución la norma ISO 15489-1 o su homóloga ecuatoriana.

11.4. Protección de los datos y privacidad de la información personal

a) El Oficial de Seguridad de la Información deberá controlar la aplicación de la política de protección de datos y privacidad de la información personal.

b) Implementar medidas técnicas y organizacionales apropiadas para gestionar de manera responsable la información personal de acuerdo con la legislación correspondiente.

c) Implementar mecanismos de carácter organizacional y tecnológico para autorización al acceso, uso e intercambio de datos personales de las personas o ciudadanos en custodia de las entidades públicas. Prima el principio que los datos personales pertenecen a las personas y no a las instituciones, éstas los custodian al amparo de la normativa legal vigente.

11.5. Prevención del uso inadecuado de servicios de procesamiento de información

a) Inventariar y aprobar el uso de los servicios de procesamiento de información por parte de la dirección de la entidad o quien esta delegue.

b) Definir y comunicar los servicios de procesamiento de información aprobados, así como los criterios para establecer el uso de estos servicios para propósitos no relacionados con la entidad sin autorización de la dirección, o para cualquier propósito no autorizado.

c) Implementar mecanismos para identificar el uso inadecuado de los servicios por medio de monitoreo u otros medios

d) Definir y especificar en las normas internas de la entidad, las acciones legales o disciplinarias cuando se compruebe el uso no adecuado de los servicios de procesamiento de información. Se considerará también lo que establece la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su Reglamento.

e) Definir la política para autorización de uso de los servicios de procesamiento de información aprobados, misma que debe ser suscrita por cada funcionario en relación de trabajo permanente o temporal, así como contratistas, asesores, proveedores y representantes de terceras partes.

f) Implementar en todos los servicios de procesamiento de información, el mensaje de advertencia que indique que el servicio al cual se está ingresando es propiedad de la entidad y que no se permite el acceso no autorizado. El usuario debe reconocer y reaccionar apropiadamente al mensaje de la pantalla para continuar con el proceso de registro de inicio. El uso de los servicios de procesamiento de información de la entidad tendrán como fin principal o exclusivo los asuntos de la institución y no los personales o de otra índole.

g) Implementar mecanismos tecnológicos y organizacionales para detectar la intrusión y evitar el uso inadecuado de los servicios de procesamiento de información. Se recomienda advertir o informar a los usuarios sobre el monitoreo y obtener su acuerdo cuando los servicios de información están abiertos a la ciudadanía o son públicos.

11.6. Reglamentación de controles criptográficos

a) Restringir importaciones y/o exportaciones de hardware y software de computadoras para la ejecución de funciones criptográficas; o diseñados para adicionarles funciones criptográficas.

b) Restringir el uso de encriptación, y especificar y documentar los ámbitos en donde se aplicarán tales procesos (ej., comunicaciones, firma de documentos, trasmisión de datos, entre otros).

c) Restringir métodos obligatorios o discrecionales de acceso por parte de las autoridades del país a la información encriptada mediante hardware o software para brindar confidencialidad al contenido.

d) Garantizar el cumplimiento con las leyes y los reglamentos nacionales antes de desplazar información encriptada o controles criptográficos a otros países.

11.7. Cumplimiento con las políticas y las normas de la seguridad

a) Revisar en intervalos regulares reportes e informes de seguridad de los sistemas de información.

b) Auditar las plataformas técnicas y los sistemas de información para determinar el cumplimiento de las normas aplicables sobre implementación de la seguridad y sus controles.

c) Revisar con regularidad en su área de responsabilidad, el cumplimiento del procesamiento de información de acuerdo con la política de la seguridad, las normas y cualquier otro requisito de seguridad. Si se determina algún incumplimiento o no conformidad como resultado de la revisión, la dirección deberá:

- Determinar la causa del incumplimiento
- Evaluar la necesidad de acciones para garantizar que no se repitan estos incumplimientos
- Determinar e implementar la acción correctiva apropiada
- Revisar la acción correctiva que se ejecutó

d) Registrar y conservar los resultados de las revisiones y las acciones correctivas llevadas a cabo por la dirección. Los directores deberán informar de los resultados a las personas que realizan revisiones independientes, cuando la revisión independiente tiene lugar en el área de su responsabilidad.

11.8. Verificación del cumplimiento técnico

a) Verificar el cumplimiento técnico bien sea manualmente (con soporte de las herramientas de software apropiadas, si es necesario) por un ingeniero de sistemas con experiencia, y/o con la ayuda de herramientas automáticas que generen un informe técnico para la interpretación posterior por parte del especialista técnico.

b) Aplicar evaluaciones de vulnerabilidad o pruebas de penetración considerando siempre el riesgo de que dichas actividades pueden poner en peligro la seguridad del sistema. Tales pruebas se deberán planificar, documentar y ser repetibles.

c) Controlar que la verificación del cumplimiento técnico sea realizado por personas autorizadas y competentes o bajo la supervisión de dichas personas.

d) Analizar los sistemas operativos para asegurar que los controles de hardware y software se han implementado correctamente. Este tipo de verificación del cumplimiento requiere experiencia técnica especializada.

e) Ejecutar o contratar pruebas de penetración y evaluaciones de la vulnerabilidad, las cuales pueden ser realizadas por expertos independientes especialmente contratados para este propósito. Ello puede ser útil para detectar vulnerabilidades en el sistema y verificar qué tan efectivos son los controles evitando el acceso no autorizado debido a estas vulnerabilidades. Las pruebas de penetración y las evaluaciones de vulnerabilidad no deben substituir las evaluaciones de riesgos.

11.9. Controles de auditoría de los sistemas de información

a) Salvaguardar los servicios de procesamiento de información y las herramientas de auditoría durante las auditorías de los sistemas de información.

b) Proteger la integridad y evitar el uso inadecuado de las herramientas de auditoría.

c) Acordar los requisitos así como el alcance de las auditorías con la dirección correspondiente.

d) Únicamente se deberá dar a los auditores acceso de lectura a la información.

e) Identificar explícitamente y poner en disposición los recursos correspondientes, para llevar a cabo las auditorías.

f) Identificar y acordar los requisitos para el procesamiento especial o adicional.

g) Monitorear y registrar todo acceso para crear un rastreo para referencia. El uso de rastreos de referencia de tiempo se debe considerar para datos o sistemas críticos.

h) Documentar todos los procedimientos, requisitos y responsabilidades de la auditoría.

i) Asegurar que la persona que realiza la auditoría sea independiente de las actividades auditadas.

11.10. Protección de las herramientas de auditoría de los sistemas de información

a) Instalar y administrar las herramientas de auditoría por parte del personal que las utiliza.

b) Los programas de software o archivos de datos de auditoría se deben separar de los sistemas de información y de desarrollo de la entidad.

c) Los archivos de seguridad y auditoría que generan los sistemas de procesamiento de información deben ser protegidos contra cualquier manipulación.

d) Mantener un estricto control de respaldos y tiempo de retención de los archivos de seguridad y auditoría de acuerdo al tipo de información y la política que se defina.

e) Mantener archivos de seguridad y auditoría en librerías de cinta, siempre que se les proporcione un nivel adecuado de protección adicional.

f) Bloquear el acceso a los archivos de seguridad y auditoría a los funcionarios no autorizados y de acuerdo al procedimiento que se defina.

GLOSARIO DE TÉRMINOS

Activo: Todo bien que tiene valor para la institución.

Ambiente de Desarrollo: tiene las siguientes características:

- En este ambiente se desarrollan los programas fuentes se almacena toda la información relacionada con el análisis y diseño de los sistemas.
- El analista o programador (desarrollador) tiene total dominio sobre el ambiente, y puede instalar componentes o actualizar versiones del software base.
- Todos los cambios del código, de software base y de componentes deben ser debidamente documentados.
- Se registra en el sistema el control de versiones que administra el "Administrador de programas fuentes".
- El desarrollador realiza las pruebas con los datos de la base de datos desarrollo.
- Cuando se considera que el programa está terminado, se lo pasa al ambiente de pruebas junto con la documentación requerida que se le entregará al implementador de ese ambiente.

Ambiente de Pruebas: tiene las siguientes características:

- Este ambiente es utilizado para realizar pruebas previas al paso a producción.
- Deberá disponer del mismo software base que el ambiente producción.
- El implementador de este ambiente recibe el programa y la documentación respectiva y realiza una prueba general con un lote de datos para tal efecto.
- El testeador realiza las pruebas con los datos de la base de datos de pruebas. Si no se detectan errores de ejecución, los resultados de las rutinas de seguridad son correctas de acuerdo a las especificaciones y se considera que la documentación presentada es completa, entonces se emite un informe favorable y se pasa el programa fuente al implementador de producción por medio del sistema de control de versiones y se le entrega las instrucciones. Caso contrario, vuelve atrás el ciclo devolviendo el programa al desarrollador, junto con un detalle de las observaciones.

Ambiente de Capacitación: tiene las siguientes características:

- Este ambiente es idéntico al ambiente de producción en su estructura, versiones de sistema y software base.
- Este ambiente será utilizado para realizar las capacitaciones respectivas a los usuarios de los sistemas.
- Este ambiente no se actualizará con la información de producción para realizar pruebas.
- Este ambiente también debe ser considerado para los respaldos de datos.

Ambiente de Producción: tiene las siguientes características:

- Es donde se ejecutan los sistemas y se encuentran los datos productivos.
- Los programas fuentes certificados se guardan en un repositorio de fuentes de producción, almacenándolos mediante un sistema de control de versiones que maneja el "administrador de programas fuentes" y donde se registran los datos del programador que hizo la modificación, fecha, hora y tamaño de los programas fuentes y objetos o ejecutables.
- El "implementador" compila el programa fuente dentro del ambiente de producción, asegurando que hay una correspondencia biunívoca con el ejecutable en producción y luego (este fuente) se elimina, dejándolo en el repositorio de programas fuentes.
- Procedimientos de la misma naturaleza que el anterior, deberán aplicarse para las modificaciones de cualquier otro elemento que forme parte del sistema; por ejemplo: modelo de datos de la base de datos o cambios en los parámetros, etc. Las modificaciones realizadas al software de base (Sistemas Operativos, Motores de bases de datos, software middleware) deberán cumplir idénticos pasos, sólo que las implementaciones las realizarán los propios administradores.
- El personal de desarrollo, como el proveedor de los aplicativos, no deben tener acceso al ambiente de producción, así como tampoco a los datos reales para la realización de las pruebas en el Ambiente de Prueba. Para casos excepcionales, se debe documentar adecuadamente la autorización, los trabajos realizados y monitorearlos en todo momento.

Comité de Gestión de Seguridad de la Información: Estará integrado al menos por: el Director Administrativo, el Responsable del área de Recursos Humanos, el Responsable del área de Tecnologías de la Información, el Responsable de Auditoría Interna y el Oficial de Seguridad de la Información. Este ente contará con un Coordinador (Oficial de Seguridad de la Información), quien cumplirá la función de impulsar la implementación del Esquema Gubernamental de Seguridad de la Información.

Confidencialidad: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Disponibilidad: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Información: Es uno de los activos más importantes de las instituciones, en las formas que esta se manifieste: textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, magnético, papel, electrónico, computadoras, audiovisual y otros.

Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Oficial de Seguridad de la Información: Será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento del Esquema Gubernamental de Seguridad de la Información. El oficial de Seguridad de la Información deberá ser un miembro independiente de las áreas de tecnología o sistemas, puesto que deberá mantener su independencia para observar las necesidades de seguridad entre la estrategia de la institución y tecnología.

Propietarios de la Información: Son los responsables de clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

Responsable del Área de Recursos Humanos: Cumplirá la función de comunicar a todo el personal que ingresa, de sus obligaciones respecto del cumplimiento del Esquema Gubernamental de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de él surjan. Asimismo, tendrá a su cargo, la difusión del presente documento a todo el personal, de los cambios que en ella se produzcan, de la implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y de las tareas de capacitación continua en materia de seguridad en coordinación con el Oficial de Seguridad de la Información.

Responsable del Área de Tecnologías de la Información: Cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la institución. Por otra parte, tendrá la función de supervisar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

Responsable del Área Legal: Verificará el cumplimiento del Esquema Gubernamental de Seguridad de la Información en la gestión de todos los contratos, acuerdos u otra documentación de la institución con sus empleados y con terceros. Asimismo, asesorará en materia legal a la institución, en lo que se refiere a la seguridad de la información.

ANEXO 4 MANUAL DEL SGSI

MANUAL DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Actualizado por:	Evelyn Arias Oficial de Seguridad de la Información	01-jul-2015	
Revisado por:	Rocío Espinosa Gerente Nacional de TI	01-jul-2015	
Aprobado por:	Ana Yépez Representante por la Dirección para el SGSI	01-jul-2015	

0. PRESENTACIÓN DE LA EMPRESA

Generalidades

- Los activos de información de la CNT EP constituyen uno de los activos de más valor, los cuales soportan su misión y visión; por lo tanto, requieren ser utilizados y manejados dentro de un adecuado entorno de seguridad, cualquiera que sea el medio y el ambiente tecnológico en el que se encuentren.
- El diseño, implantación y operación del Sistema de Gestión de Seguridad de la información (SGSI) de la CNT EP está directamente relacionado con sus necesidades, objetivos organizacionales y direccionamiento estratégico, estructura, alcance y requerimientos de seguridad.
- El Sistema de Gestión de Seguridad de la información está orientado a definir los aspectos necesarios para establecer, operar, mantener y dirigir un sistema efectivo para el tratamiento seguro de la información de la CNT EP.

Descripción resumida de la Corporación Nacional de Telecomunicaciones CNT EP

La Corporación Nacional de Telecomunicaciones CNT EP es la empresa pública de telecomunicaciones del Ecuador creada el 14 de enero de 2010, opera servicios de telefonía fija local, regional e internacional, acceso a internet estándar y de alta velocidad, televisión satelital y telefonía móvil en el territorio nacional ecuatoriano.

Estructura organizacional de la CNT EP

A continuación se presenta la estructura organizacional de la CNT EP para llevar a cabo sus actividades y cumplir con sus objetivos estratégicos:

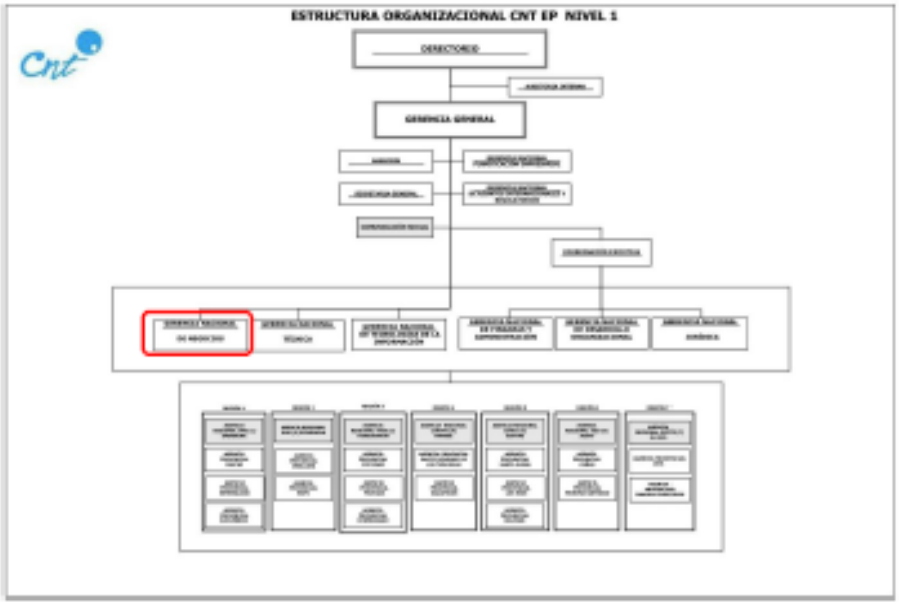


Ilustración 1. Estructura Organizacional. Fuente: Página web oficial de la CNT EP.

En esta estructura organizacional se puede identificar la Gerencia Nacional de Negocios que depende directamente de la Gerencia General de la CNT EP, la cual hace parte del alcance del SGSI, que tiene relación con diferentes grupos de interés (Clientes, Colaboradores de la CNT EP, Proveedores, Entes regulatorios o de control internos y externos) que son definidos para cada uno de los procesos de la Entidad; tiene relación también con otras gerencias expuestas en el organigrama ya que estas son un soporte dentro de sus actividades. En el Anexo 1 Partes interesadas del SGSI se describen las partes interesadas del SGSI y los requisitos de seguridad de la información definidos por estos.

Mapa de procesos de la CNT EP

Para cumplir con los propósitos de la CNT EP, se definieron procesos Core del negocio y procesos Soporte del negocio, dentro de la Gerencia Nacional de Negocios se cuentan con estos procesos que están divididos como se muestran en las siguientes figuras:

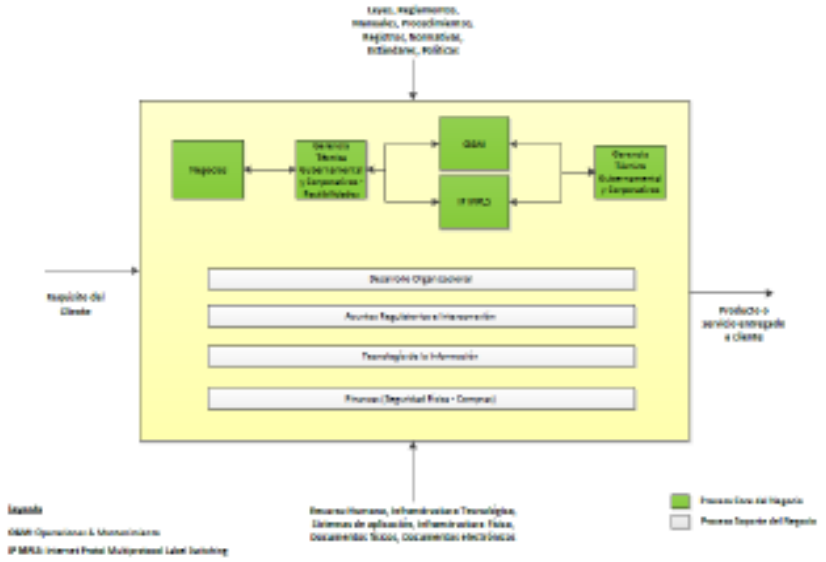


Ilustración 2. Mapa de Procesos de Venta e instalación de productos y servicios de datos e Internet para clientes corporativos en el Distrito Metropolitano de Quito. Fuente: Desarrollo Organizacional.

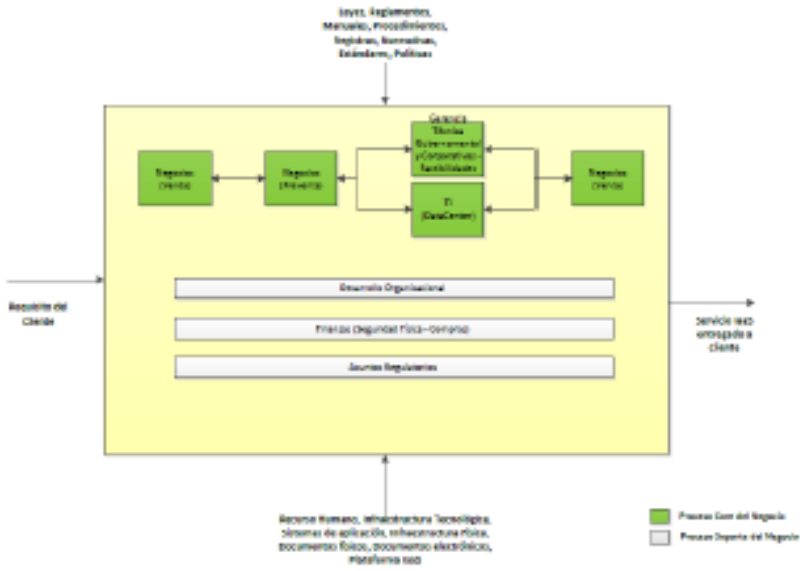


Ilustración 3. Mapa de Procesos de Venta y aprovisionamiento de infraestructura como servicio (IaaS) en un esquema de Cloud Computing para clientes gubernamentales y corporativos en el Distrito Metropolitano de Quito. Fuente: Desarrollo Organizacional.

Alcance del SGSI

Los procesos definidos dentro del alcance del SGSI de la CNT EP son:

- Proceso de venta e instalación de productos de servicios de datos (servicios con enlaces dedicados para transmisión de datos a través de la red de CNT EP) e Internet (servicios de conexión a Internet a través de la red de CNT EP) para clientes corporativos en el Distrito Metropolitano de Quito.
- Proceso de venta y aprovisionamiento de Infraestructura como Servicio (IaaS) (servicios dedicados de Centro de Datos Virtual para procesamiento de datos a través de la plataforma de virtualización de CNT EP) en un esquema de Cloud Computing para Clientes Gubernamentales y Corporativos en el Distrito Metropolitano de Quito.

La Corporación Nacional de Telecomunicaciones CNT EP cuenta con oficinas para el Distrito Metropolitano de Quito en las cuales se encuentran los procesos del alcance del SGSI se encuentran ubicadas en las siguientes direcciones:

Oficina Central:	Amazonas y Japón	Edificio Vivaldi
Oficinas:	Eloy Alfaro y Nueve de Octubre	Edifico Doral
	Gaspar de Villarroel y Amazonas	Edificio Iñaquito
	Cordero y 9 de Octubre	Edificio Droira
	Av. De los Shyris y Tierra	Edificio Tierra

Tecnología de la CNT EP

La CNT EP cuenta con sistemas de información y servidores donde reposan los activos más importantes de los procesos del alcance del SGSI.

Los servidores donde se encuentran estos sistemas de información son propiedad de la CNT EP y se encuentran en los centros de datos ubicados en las instalaciones del Edificio Iñaquito Piso 1.

Partes interesadas al SGSI

Los procesos definidos en el alcance del SGSI han identificado las siguientes partes interesadas de acuerdo a los requisitos en seguridad de la información que existen para la información que es gestionada a través de los servicios que prestan:

PARTES INTERESADAS	DESCRIPCIÓN
CLIENTES	Clientes corporativos (gobierno, vip, ISP's carriers y pymes) y gubernamentales.
CIUDADANÍA – SOCIEDAD	Sociedad en general, se encuentra una afectación cuando se tienen nuevos proyectos en CNT que tienen que ver con aspectos geográficos
COLABORADORES	Empleados de CNT.
ENTES DE REGULACIÓN Y CONTROL INTERNOS	Gerencia de Calidad y Procesos. Asuntos Regulatorios Gerencia Nacional Jurídica (Procesos de Contratación)
ENTES DE REGULACIÓN Y CONTROL EXTERNOS	Contraloría General del Estado. Arcotel (Permisos de frecuencias y homologaciones de equipamiento, cantidad de servicios) SNAP (Coordinación de políticas públicas sobre contratación de tecnología y telecomunicaciones) MINTEL (Ente coordinador, CNT pertenece al MINTEL como sector estratégico) Asamblea (Emisión de leyes) SENAIN (Secretaría Nacional de Inteligencia) Fiscalía General de la Nación
PROVEEDORES	Infraestructura, SW, HW y Servicios (Consultorías y horas técnicas)
OTROS	Gerencia Nacional Financiera (Costos - Presupuestos) Gerencia Nacional Técnica (Implementación de Soluciones) Gerencia General (Custodio de los contratos originales físicos) Gerencia Nacional de TI (Sistemas Transaccionales) Gerencia Nacional de Negocios (Desarrollo de productos, compra de terminales, planificación operativa) Gerencia Desarrollo Organizacional (Elaboración de procesos, Contratación/Acuerdos de Confidencialidad) Gerencia de Planificación Estratégica Activación de Servicios Desempeño de Red

Ilustración 4. Partes interesadas al SGSI de la CNT EP.

1. OBJETO Y CAMPO DE APLICACIÓN

1.1. Generalidades

Este Manual especifica los requisitos del Sistema de Gestión de la Seguridad de la Información de la Corporación Nacional de Telecomunicaciones CNT EP (en adelante la CNT EP o la Corporación), los mismos que cumplen con los requisitos de los clientes, así como con los legales y reglamentarios del país.

Además proporciona las guías para la prevención de las no-conformidades y los procesos de mejora continua.

1.2. Aplicación

Debido a la naturaleza del negocio de la CNT EP, así como al alcance del Sistema de Gestión de la Seguridad de la Información, la Corporación ha declarado conformidad con la norma ISO 27001:2013 e implementado sin excepción los requisitos del

numeral 4 al 10. Sin embargo, ha excluido ciertos controles del Anexo A de la Norma ISO 27001:2013. El detalle se encuentra en el documento "Declaración de Aplicabilidad", el mismo que ha sido revisado y aceptado por el representante de la Gerencia General.

1.3. Declaración de Aplicabilidad

La Declaración de Aplicabilidad (Anexo 2) menciona los controles existentes al momento de definir el Sistema de Gestión de Seguridad de la Información de la CNT EP y realizar el análisis de riesgos, así como los controles y objetivos de control que han sido seleccionados con base en el análisis y evaluación de riesgos, en los requerimientos de seguridad identificados y por ende, en el las definiciones dadas en el plan de tratamiento del riesgo.

Estos controles están basados en los controles definidos en la norma ISO/IEC 27001:2013 Anexo A.

La declaración de aplicabilidad debe ser documentada y actualizada cuando cambian las condiciones de la CNT EP, los procesos, la infraestructura tecnológica, el análisis de riesgos, entre otros.

2. NORMAS PARA CONSULTA

Las normas en las cuales se ha basado la CNT EP son aquellas definidas en el capítulo 2 de la Norma ISO 27001:2013.

3. TÉRMINOS Y DEFINICIONES

Para los fines de este Manual, se aplican los términos y definiciones dadas en la Norma ISO 27000:2014, además de las que se encuentran detalladas en cada una de las normativas y procedimientos que son parte del Sistema de Gestión de Seguridad de la Información.

4. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

4.1. Requisitos Generales

La CNT EP ha establecido, documentado, implementado y mantiene un Sistema de Gestión de la Seguridad de la Información, el mismo que es revisado y mejorado continuamente conforme con los requisitos de la Norma ISO 27001:2013.

4.2. Establecimiento y Gestión del SGSI (Pirámide SGSI)

4.2.1. Política del SGSI

La CNT EP, enmarcando sus actividades bajo los requerimientos que como empresa pública debe cumplir, trabaja para brindar servicios de telecomunicaciones manteniendo un nivel alto de protección de la información que maneja a través de su Sistema de Gestión de la Seguridad de la Información, protegiéndola mediante la pertinente gestión de riesgos, promoviendo una cultura de seguridad de la información, el cumplimiento de la normatividad vigente, requisitos legales, generando una oportuna gestión a los incidentes y aplicando mejores prácticas aplicadas a través de controles de seguridad, y garantizar la confidencialidad, integridad y disponibilidad de la información y los activos que la resguardan. La Corporación garantiza el cumplimiento, mantenimiento y mejora continua de dicho Sistema dotando de los medios y recursos necesarios e instando a todo el personal para que asuma este compromiso.

4.2.1.1. Objetivos de seguridad de la información

Los objetivos de seguridad de la información del SGSI concretan y materializan la Política de Seguridad de la Información en propósitos alcanzables y tangibles para los procesos del alcance del SGSI.

Para definir los objetivos de Seguridad de la Información se tiene en cuenta el entendimiento de la estrategia de la CNT EP.

Teniendo en cuenta lo anterior los objetivos de seguridad de la información están alineados con la política de seguridad de la información y la estrategia de CNE EP, y son los siguientes:

- Contribuir al logro de los objetivos de negocio de CNT EP, al mismo tiempo que se administran los riesgos de Seguridad de la Información en los activos de información de la Corporación.
- Alinear la orientación estratégica de Seguridad de la Información con la estrategia del negocio de la Empresa a través de la identificación y clasificación de los activos de información de la Corporación con base en su impacto en los atributos claves del negocio.

- Apoyar a hacer crecer la percepción de CNT EP como una Empresa que responde a los requerimientos de Seguridad de la información de sus partes interesadas (colaboradores, clientes, proveedores, los entes de regulación y control) mediante las revisiones al SGSI e implementaciones de controles de seguridad en los activos de información que estas acceden y el desarrollo de iniciativas de sensibilización al interior de la Corporación.
- Fortalecer el correcto y eficiente funcionamiento de los servicios informáticos brindados a clientes externos e internos de la CNT EP, tratando efectivamente los incidentes de seguridad con el fin de identificar causas y realizar acciones de corrección para la mejora continua del sistema de gestión de seguridad de la información.
- Mejorar la gestión de la Seguridad de la información de CNT EP mediante la implementación en sus activos de información de controles de seguridad diseñados acorde con las buenas prácticas y la norma ISO/IEC 27001.
- Objetivos que han sido obtenidos con base a la Política del Sistema de Gestión de Seguridad de la información (SGSI), definida en el numeral 4.2.1.

4.2.2. Estructura organizacional de seguridad de la información

La estructura organizacional de la Seguridad de la información en la CNT EP se describe en la Normativa de Roles y Responsabilidades de Seguridad de la información.

4.2.2.1. Enfoque de Riesgos

Como parte de la implementación del Sistema de Gestión de la Seguridad de la información en la CNT EP, se utiliza el Procedimiento de Identificación, Clasificación y Evaluación de los Activos de información y la Metodología de Evaluación de Riesgos de Seguridad de la información, que permite:

1. Identificar los activos de información dentro del alcance del SGSI[1].
2. Clasificar la información con base en una identificación del nivel de impacto a la confidencialidad, disponibilidad e integridad sobre los activos de información
3. Clasificar los activos de información identificados.
4. Identificar el contexto estratégico de CNT EP.
5. Seleccionar los activos críticos de acuerdo con su nivel de impacto.
6. Identificar el Universo de Amenazas y Vulnerabilidades.

[1] Las actividades del 1 al 3 se generan ejecutando el Procedimiento de Identificación, Clasificación y Evaluación de los Activos de información, las demás se generan de ejecutar la Metodología de Evaluación de Riesgos de Seguridad de la información.

7. Definir y aplicar una lista de chequeo de controles
8. Determinar la probabilidad de ocurrencia de los riesgos (Nivel de Vulnerabilidad)
9. Analizar y evaluar los riesgos
10. Determinar la aceptación del riesgo
11. Identificar y evaluar opciones de tratamiento de riesgos
12. Identificar posibles controles a implementar para el tratamiento de los riesgos
13. Seleccionar controles a implementar para el tratamiento de riesgos inaceptables

Esta metodología está alineada con la gestión de riesgo estratégico de la organización, para el establecimiento y mantenimiento del SGSI de CNT EP.

4.3. Requisitos de Documentación

4.3.1. Generalidades

La documentación del Sistema de Gestión de la Seguridad de la Información incluye los elementos que se detallan en la siguiente Pirámide de la documentación:

Para controlar la información documentada del SGSI se cuenta con el Procedimiento para el control de documentos y registros del SGSI.

4.3.2. Manual del Sistema de Gestión de Seguridad de la Información (Manual del SGSI)

El Manual de Gestión de la Seguridad de la Información de la CNT EP expresa el compromiso en materia de Seguridad como parte de la Visión y Estrategia Empresarial de la CNT EP. En él se describen las disposiciones generales tomadas para asegurar la confidencialidad, integridad y disponibilidad de la información, así como la prevención de no conformidades y la aplicación de acciones para evitar su recurrencia.

En el Manual del Sistema de Gestión de la Seguridad de la Información se presenta además, la Política del SGSI así como su alcance *(ver Sección 0 de este manual)*, todo ello conforme se establece en la Norma ISO 27001:2013.

Al Manual del Sistema de Gestión de la Seguridad de la Información se subordinan la Política de Seguridad de la Información y las demás Normativas, Procedimientos, Instructivos, Manuales, Estándares y Registros conforme se lo señala en el numeral 4.3.1 de este manual.

4.3.3. Control de Documentos

De acuerdo a lo requerido por la Norma ISO 27001:2013, todo documento debe:

- Ser aprobado y formalizado antes de ser publicado
- Ser revisado, actualizado y re aprobado si es necesario
- Tener identificado todo cambio o actualización
- Ser legible e identificable
- Estar disponible para quienes lo requieran
- Ser distribuido de forma controlada
- Si es identificado como obsoleto, deberá ser retirado

4.3.4. Control de Registros

Los registros requeridos por el Sistema de Gestión de la Seguridad de la Información son controlados. Estos registros son mantenidos para proporcionar la evidencia de conformidad con los requisitos y con la operación eficaz del SGSI, por lo cual se mantienen legibles, identificables y recuperables según su periodo de retención. Los registros que forman parte del SGSI son de uso interno.

5. RESPONSABILIDAD DE LA DIRECCIÓN

5.1. Compromiso de la Dirección

La Alta Dirección (Gerente General y Comité de Dirección) demuestra su compromiso comunicando la importancia de cumplir con los requisitos impuestos dentro de los distintos controles que forman parte del SGSI, realizando las Revisiones de la Dirección y asegurando la disponibilidad de los recursos necesarios para continuar operando y mejorando el SGSI.

5.2. Gestión de Recursos

5.2.1. Provisión de Recursos

La CNT EP, a través del presupuesto aprobado por el Directorio, asegura la provisión de recursos esenciales para implementar, operar, revisar, mantener y mejorar el SGSI. Los recursos asignados son gente, infraestructura y recursos financieros.

5.2.2. Formación, toma de conciencia y competencia

La CNT EP, con el objeto de contar con el personal competente, de acuerdo a los requerimientos de Seguridad de la información, realiza charlas frecuentes y actualizadas con el objetivo de concientizar y capacitar a sus colaboradores.

El Oficial de Seguridad de la información realiza un Plan de Capacitación Permanente, el cual es revisado anualmente para asegurar su pertinencia.

Los métodos utilizados dependen de la planificación, por lo cual puede hacerse uso de cualquier medio tecnológico, físico o publicitario que permita llegar a la comunidad de la CNT EP, considerando también que se deben ejecutar evaluaciones al personal capacitado para medir su nivel de asimilación del conocimiento y para determinar el grado de compromiso que tienen con la Seguridad de la información de la CNT EP.

6. AUDITORÍAS INTERNAS

La CNT EP, ha elaborado el Plan de Auditoría del SGSI concebido para ejecutar una revisión semestral de tipo muestreo de los distintos controles de la Norma ISO 27001:2013, llegando en un año a revisar todos los controles de la norma.

Las auditorías internas buscan determinar si el Sistema de Gestión de la Seguridad de la información se mantiene conforme con los requisitos de la Norma ISO 27001:2013, y que ha sido eficazmente implantado, mantenido y operado por parte de los colaboradores de la CNT EP.

CNT EP cuenta con el procedimiento de Auditorías Internas al SGSI para cumplir con este requisito de la norma ISO 27001:2013.

7. REVISIÓN DEL SGSI POR LA DIRECCIÓN

7.1. Generalidades

La Gerencia General de la CNT EP revisa anualmente el SGSI para determinar su idoneidad, suficiencia y eficacia continuas ya que puede existir la necesidad de mejorar o implementar cambios en el SGSI, incluyendo las Políticas, Objetivos de Seguridad, Normativas y/o Procedimientos aprobados anteriormente. Adicional a esto, durante el año se realizan por lo menos 3 revisiones de seguimiento al SGSI por parte del Representante por la Dirección.

7.2. Información para la revisión

Los parámetros a tener en cuenta para la revisión incluyen:

- Acciones de seguimiento de las anteriores revisiones del sistema
- Cambios que afecten al SGSI
- Los resultados de las auditorías del SGSI
- Situación de las acciones correctivas y preventivas
- Cumplimiento de los objetivos de seguridad de la información
- Retroalimentación del personal enmarcado en el alcance del SGSI
- Técnicas, productos o procedimientos que pudieran utilizarse para mejorar el SGSI
- Resultados de la valoración de riesgos y estado del plan de tratamiento de riesgos
- Vulnerabilidades o amenazas no tratadas adecuadamente
- Recomendaciones u oportunidades para la mejora continua
- Documentación del SGSI

7.3. Resultados de la Revisión

El resultado de la revisión por la Gerencia incluye acciones con relación a la mejora del SGSI y sus componentes, incluyendo la metodología de evaluación de riesgos y el plan de tratamiento de riesgos.

Los resultados de la revisión son registrados en informes emitidos a la Gerencia General. En estos, se provee información suficiente para permitir dar seguimiento y trazabilidad de las distintas revisiones, de tal forma que asegure su continuidad y agregue valor a la organización considerando eventuales cambios a los requisitos del negocio, requisitos de seguridad, el alcance del SGSI, requisitos legales y niveles de aceptación de riesgos.

Para la revisión del SGSI por la Dirección se utilizará el Formato de Revisión por la Dirección del SGSI. (Anexo 3).

8. MEJORA DEL SGSI

8.1. Mejora Continua

La CNT EP, ha establecido su SGSI como un modelo que le permita mejorar continuamente incluyendo una política del SGSI, amparada por la Política de Seguridad de la información y demás controles tanto técnicos como no técnicos así como los resultados de las auditorías y demás revisiones que continuamente arrojan no conformidades u oportunidades de mejora, las mismas que se ven traducidas en acciones preventivas y correctivas. Para esto CNT cuenta con el procedimiento Acciones Correctivas y Acciones Preventivas.

8.2. Acción Correctiva

La CNT EP, ha definido un proceso para la realización de acciones correctivas que busca eliminar las causas de las no conformidades para prevenir la recurrencia.

8.3. Acción Preventiva

La CNT EP, se preocupa por identificar no conformidades potenciales y sus causas por medio de revisiones periódicas realizadas por parte del Oficial de Seguridad de la información y su equipo de trabajo (Analistas de Seguridad de la información). Dichas revisiones se ejecutan según lo indicado en cada procedimiento que forma parte del SGSI.

9. ANEXOS

9.1. Anexo 1. Partes interesadas del SGSI

Este anexo incluye las partes interesadas al SGSI, los requisitos de las partes interesadas en cuanto a seguridad de la información y las interfaces de las actividades realizadas por los procesos del alcance del SGSI y las que realizan otras organizaciones.

9.2. Anexo 2. Declaración de Aplicabilidad del SGSI

Este anexo incluye los controles existentes al momento de definir el Sistema de Gestión de Seguridad de la Información de la CNT EP y realizar el análisis de riesgos, así como los controles y objetivos de control que han sido seleccionados con base en el análisis y evaluación de riesgos, en los requerimientos de seguridad identificados y por ende, en el las definiciones dadas en el plan de tratamiento del riesgo.

9.3. Anexo 3. Formato de Revisión del SGSI por la Dirección

Este anexo incluye los temas a tratar para la revisión del SGSI por la Dirección y las acciones tomadas para mejorar el sistema de gestión.

10. REGISTRO DE ACTUALIZACIONES

En el cuadro siguiente se deben identificar todas las actualizaciones realizadas sobre el presente manual.

CAMBIO No.	SECCIÓN	HOJA	CONCEPTO	AUTORIZADO POR	FECHA
1	0	1 y 2	Alcance del SGSI, Dirección oficina Central	Evelyn Arias	23 – oct - 2014
2		Todas	Etiquetamiento de Clasificación - Interno	Evelyn Arias	30 – oct - 2014
3	0	2	Alcance del SGSI, Dirección de Oficina Tierra	Evelyn Arias	30 – oct - 2014
4	4	6	Requisitos Generales - Continuamente Mejorado cambia a Mejorado Continuamente	Evelyn Arias	30 – oct - 2014
5	4.2.1.2	6	Enfoque de Riesgos - Se aumenta en metodología de valoración de riesgos "organizacionales"	Evelyn Arias	30 – oct - 2014
6	4.2.1.2	6 y 7	Enfoque de Riesgos - Alineación a la gestión de riesgo estratégico de la organización	Evelyn Arias	30 – oct - 2014
7	Integral	Todas	Mejoras de contexto y correcciones generales	Evelyn Arias	30 – mar – 2015
8	Integral	Todas	Mejoras de contexto y correcciones generales	Evelyn Arias	01 – jul – 2015

ANEXO 5 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI-NOC

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI-NOC	
Autor: Luis Fernando Molina Batallas	
Empresa: Corporación Nacional de Telecomunicaciones CNT EP	
Área: Centro de Operaciones de Redes NOC	
COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	
PERSONA ASIGNADA	**ROL DESEMPEÑADO**
ING. OSCAR CORREA	DIRECTOR ADMINISTRATIVO
INGA. MERY ALARCÓN	COORDINADOR
ING. ANDRÉS SALAZAR	OFICIAL DE SEGURIDAD DE LA INFORMACIÓN
ING. JORGE BUENO	RESONSABLE DE RECURSOS HUMANOS
ING. JORGE JARA	RESPONSABLE DEL ÁREA DE TECNOLOGÍAS
ING. JORGE TOBAR	RESPONSABLE DE ACTIVOS
ING. EDGAR ALARCÓN	RESPONSABLE DE AUDITORÍA INTERNA
POLÍTICAS PROPUESTAS	
DOMINIO	**POLÍTICAS**
Políticas de Seguridad de la Información	Se crea el documento “Sistema de Gestión de Seguridad de la Información SGSI-NOC”
	El documento es administrado por el comité de seguridad de la información

	Se requiere realizar revisiones periódicas del documento
Organización de la Seguridad de la información	Se selecciona el comité de seguridad de la información
	Valoración de activos
	Determinación del riesgo
	El personal del área del NOC tiene solo acceso a la información disponible
	El acceso a la información por personas fuera del área debe de ser documentado y autorizado
	Se debe de tener un registro de todos los eventos ocurridos
	Toda modificación en los programas, utilitarios y herramientas de uso dentro del área debe de ser solicitada por la persona que desea realizar dicho cambio
	Todo cambio debe de ser documentado desde su solicitud hasta su implementación
	Se requiere mantener contacto con organizaciones públicas y privadas especializadas en seguridad de la información
	Se recomienda realizar revisiones independientes y periódicas del sistema de gestión de seguridad de la información
Gestión de los Activos	Se dispondrá de un inventario de activos
	Capacitar al personal que desconoce la gestión de la seguridad de la información
	Los servicios de correo electrónico institucional e internet deben utilizarse para

	las funciones específicas del área y no deben utilizarse para ningún otro fin
Seguridad de los Recursos Humanos	Políticas gestionadas por el área de recursos humanos DEO
	Se debe de firmar acuerdos de confidencialidad
	Las conexiones de equipos, sistemas o recursos que no pertenezcan al área y que requieran conectarse con la red interna del área necesitan acuerdos certificados
Seguridad Física y del Entorno	Se propone implementar un sistema cerrado de vigilancia
	Se debe de tener sistemas contra incendios en el área
	Se requieren mecanismos de control de acceso para el área
	Toda persona ajena al área que desee ingresar debe de registrarse informando el propósito de su visita
	Todo personal que labora dentro del área tendrá que hacer uso de su credencial de trabajo
	Se debe de limitar el acceso solo a personal autorizado a las zonas de acceso al cableado físico de energía, transmisión y recepción de datos
	Se debe de registrar el ingreso y salida de todos los equipos físicos
	Los equipos no deben moverse o reubicarse sin previa autorización
	Todos los equipos deben someterse a

	mantenimientos periódicos
	Respecto al retiro de equipos del área se requiere una previa autorización
Gestión de Comunicaciones y Operaciones	Se documentará la gestión de los procesos realizados dentro del área
	Toda la información que concierne al uso de la red de datos utilizada internamente dentro del área como es la topología física de red, direccionamiento ip, medidas de seguridad, etc; debe clasificarse como información confidencial y reservada
	La salida de información utilizada por el área hacia otras entidades debe de cumplir con acuerdos de confidencialidad
	Se debe de verificar las características de los sistemas de información
	Se prohibe el uso de software no autorizado
	Se gestionará el registro de auditorías
	Toda la información utilizada y generada dentro del área debe de ser respaldada
	Todo cambio realizado dentro del área será registrado e identificado
Control de Acceso	Las políticas de seguridad de control de acceso son gestionadas por el área de sistemas SIS
	Las contraseñas deben de contener caracteres alfanuméricos y como mínimo deben de estar conformadas de 8 caracteres
	Las contraseñas de los usuarios deben de cambiarse cada 120 días

	Las contraseñas de los administradores deben de cambiarse cada 90 días
	No debe de reutilizarse contraseñas antiguas
	Cada usuario debe disponer de un nombre de usuario y contraseña única
	Las contraseñas deben tener una fecha de caducidad definida en base a la sensibilidad de la información a proteger
	Se deben tener definidos los perfiles de usuario de acuerdo a la función y cargo de los usuarios
	Todos los equipos se bloquearán después de 10 min de inactividad
	Se controlará el acceso a las aplicaciones y herramientas utilizadas dentro del área
Adquisición, Desarrollo y Mantenimiento de sistemas de Información	Ningún personal del NOC debe suministrar cualquier información de la institución a ningún ente externo sin la autorización respectiva
	Todo el personal debe firmar y renovar cada año, un acuerdo de confidencialidad y buen manejo de la información
	La persona que detecte el mal uso de la información está en la obligación de reportar el hecho
	Se requiere analizar los medios y comunicaciones utilizadas para la transferencia de información especialmente los de salida de información
Gestión de los Incidentes de la Seguridad de la Información	La gestión de incidencias actualmente aplicada en el área del NOC no tendrá cambios en sus políticas y procedimientos

	utilizados
	Se tiene como prioridad la atención y solución inmediata de los problemas reportados por todos los clientes corporativos y gubernamentales a nivel nacional
Gestión de la Continuidad del Negocio	Se dispondrá de equipamiento de respaldo ubicado en otra sucursal de la empresa en caso de siniestro o desastre natural
	La información será respaldada en la base de datos utilizada en el NOC así como en la base de datos administrada por el departamento de sistemas SIS de la empresa
	Se realizará pruebas del plan de contingencia elaborado
Cumplimiento	Estas políticas son gestionadas por la gerencia nacional jurídica
	Se definen los documentos de registro
	El software utilizado debe garantizar la integridad de los datos
	Se debe crear una cultura en los usuarios de la institución sobre las implicaciones del uso de software ilegal
	Se mantendrá un inventario de las licencias de software de la empresa
	Cualquier alteración en la configuración del hardware (procesador, memoria, tarjetas adicionales, etc.) debe ser autorizado por el personal responsable de los recursos
	El movimiento y/o re-ubicación de equipos (PC, servidores, equipamiento activo) debe documentarse y estar debidamente

	autorizado
	Se dispondrá de un listado de usuarios autorizados, especificando nombre, apellidos y cargo que ocupa en la institución, así como los servicios para los que está autorizado