ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

PROPUESTA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA CORPAIRE

TESIS PREVIA A LA OBTENCIÓN DEL GRADO DE MAGISTER (MSc.) EN GESTIÓN DE LAS COMUNICACIONES Y TECNOLOGÍAS DE LA INFORMACIÓN

KLÉVER IVÁN TIPÁN GUAYTA
klever_ivan@hotmail.com

DIRECTOR: MSc. ING. GUSTAVO SAMANIEGO
gustavo.samaniego@epn.edu.ec

Quito, Enero 2012

DECLARACIÓN

Yo Kléver Iván Tipán Guayta, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Kléver Iván Tipán Guayta

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Kléver Iván Tipán Guayta, bajo mi supervisión.

Msc. Ing. Gustavo Samaniego
DIRECTOR DE PROYECTO

AGRADECIMIENTO

A mi familia que comprenden mi esposa e hijos, mis padres y hermanos; y todos quienes supieron brindarme todo el apoyo para culminar mis estudios. A ellos que día a día con su amor, paciencia y sobre todo palabras de aliento hicieron que finalice un peldaño más de mi profesión.

A mi estimado director de tesis, Ing. Gustavo Samaniego, por la gran colaboración y ayuda para la realización de el presente Proyecto de Titulación. Muchas gracias!!!

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El contenido de este proyecto de tesis inicia con una Caracterización de la Situación Actual de la CORPAIRE. Se analiza la situación actual de la Corporación respecto a Políticas de Seguridad de la Información. También se describe información corporativa desde varios puntos de vista como parte fundamental en la estructura institucional. De igual manera se describe la organización de la Corporación y del Departamento de Tecnología de la misma.

En el segundo capítulo se realiza el Análisis de Riesgos de Seguridad de la Información. Aquí se realiza un análisis comparativo de tres marcos de trabajo utilizados para Análisis y Evaluación de Riesgos, el resultado de este análisis selecciona a la Norma ISO/IEC 27005:2008 como marco de trabajo para realizar el Análisis de Riesgos de Seguridad de la Información. Con el marco de trabajo seleccionado se realiza la Valoración y Evaluación del Riesgo.

En el tercer capítulo se elaboran las Políticas de Seguridad de la Información. Se inicia con un análisis comparativo de tres marcos de trabajo utilizados para la elaboración de las políticas, este proceso justifica la selección de las plantillas de SANS Security Policy Project como marco de trabajo para la declaración de las Políticas de Seguridad de la Información.

En el cuarto capítulo se realiza la Evaluación de la Aplicabilidad y Funcionalidad de esta propuesta de políticas desde el punto de vista legal, económico, técnico, organizacional y operativo.

Finalmente en el quinto capítulo se plasman las conclusiones y recomendaciones sobre esta tesis.

CAPÍTULO 1

CARACTERIZACIÓN DE LA SITUACIÓN ACTUAL DE LA CORPAIRE

1.1 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Generalidades

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

Las Políticas de Seguridad de la Información protegen a la Corporación de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la organización.

Es importante que los principios de las Políticas de Seguridad de la Información sean parte de la cultura organizacional. Para esto, se debe asegurar un compromiso manifiesto de las máximas autoridades de la corporación para la difusión, consolidación y cumplimiento de las políticas.

Para la adecuada gestión de las Tecnologías de la Información y Comunicaciones, es necesario desarrollar las Políticas de Seguridad de la Información que permitan formalizar los esfuerzos de una organización para que la información cumpla los principios básicos de la seguridad como son la Integridad, Disponibilidad y Confidencialidad.

Objetivo

Proteger los recursos de información de la Corporación y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas deliberadas o accidentales, con el fin de asegurar el cumplimiento de la Integridad, Disponibilidad y Confidencialidad de la información.

Asegurar la implementación de las medidas de seguridad comprendidas en estas Políticas de Seguridad de la Información, identificando los recursos y el presupuesto correspondiente.

Mantener las Políticas de Seguridad de la Información de la corporación actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

Alcance

Estas Políticas de Seguridad de la Información se aplican en todo el ámbito de la CORPAIRE, a sus activos de información y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Responsabilidad

Todos los Jefes o Directores de Área sea cual fuere su nivel jerárquico son responsables de la implementación de estas Políticas de Seguridad de la Información dentro de sus áreas de responsabilidad, así como del cumplimiento de las mismas por parte de su equipo de trabajo.

Las Políticas de Seguridad de la Información es de aplicación obligatoria para todo el personal de la CORPAIRE, cualquiera que sea el área a la que pertenece y cualquiera sea el nivel de las tareas que desempeñe.

1.1.1 TÉRMINOS Y DEFINICIONES DE SEGURIDAD DE LA INFORMACIÓN

Política de Seguridad. Es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información. Contiene la definición de la seguridad de la información bajo el punto de vista de cierta entidad. Debe ser fácilmente accesible de forma que los empleados estén al tanto de su existencia y entiendan su contenido. Se debe designar un

propietario que será el responsable de su mantenimiento y actualización a cualquier cambio que se requiera. [1]

Las políticas no deben ser numerosas, deben ser apoyadas y aprobadas por las directivas de la corporación y deben ofrecer direccionamientos a toda la organización. Las políticas son obligatorias y la incapacidad o imposibilidad para cumplir una política exige que se apruebe una excepción. El hecho de desconocer la política no le exime de responsabilidad o sanción establecida.

Confidencialidad. Garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Integridad. Salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Disponibilidad. Garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Autenticidad. Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Auditabilidad. Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

Protección a la duplicación. Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

[1] Tomado de: http://es.wikipedia.org/wiki/Pol%C3%ADticas_de_seguridad

No repudio. Se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Legalidad. Se refiere al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

Confiabilidad de la Información. La información que se genera sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Información. Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Sistema de Información. Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Tecnología de la Información. Se refiere al hardware y software operados por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

1.1.2 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA CORPAIRE.

Actualmente no existen Políticas de Seguridad de la Información en la CORPAIRE, que permitan validar que la información sea correcta, completa y esté siempre a disposición, además de que sea utilizada únicamente por aquellos que tienen autorización y que los recursos tecnológicos sean aprovechados de manera adecuada y óptima; es así que se requiere diseñar

de manera formal un documento de Políticas, de tal forma que interactúe con los procesos de la institución y logre apoyar los objetivos estratégicos.

Para el desarrollo de las Políticas de Seguridad de la Información para la corporación se necesita de un entendimiento cuidadoso de la organización. Para aquello se debe considerar los objetivos estratégicos, reglas, regulaciones y leyes a las cuales la CORPAIRE está sujeta. Por tal motivo se requiere determinar el ambiente donde se implementará las políticas y describir el proceso de desarrollo de estas políticas tomando en cuenta los marcos de trabajo a utilizar.

1.1.3 RAZONES PARA ELABORAR LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA CORPAIRE

A continuación algunas razones por las cuales se recomienda elaborar las políticas de seguridad de la información para la CORPAIRE:

1. Cumplir con regulaciones definidas por la Dirección General de Informática del Distrito Metropolitano de Quito.
2. Alinear los objetivos específicos de las Tecnologías de la información con los objetivos estratégicos de la institución
3. Establecer el uso de mejores prácticas referente a la Gestión de las Tecnologías de la Información en las actividades diarias.
4. Hacer más eficiente el trabajo de los empleados.
5. Disponer de una herramienta al momento de tomar decisiones.

1.2 INFORMACIÓN CORPORATIVA

Para tener una mayor comprensión del ambiente donde se implemente las Políticas de Seguridad de la Información, es necesario describir la información corporativa como parte fundamental en la estructura institucional, y tiene que ver con:

- Personas
- Infraestructura Tecnológica
- Revisión Técnica Vehicular
- Monitoreo del Aire
- Leyes y ordenanzas municipales

Dicha información puede estar presente de manera electrónica o simplemente en papeles, esta influye de manera directa en todos los procesos internos de la corporación, así como de manera indirecta con varias entidades del medio exterior.

Esta información es de vital importancia para el desarrollo de las actividades y operaciones de la CORPAIRE, y se la caracterizará desde los puntos de vista técnico, legal e institucional.

1.2.1 PUNTO DE VISTA TÉCNICO

Principalmente se tratarán los temas tales como medios de almacenamiento, gestión de la información y acceso a la información.

Medios de Almacenamiento. La mayor parte de la información de la CORPAIRE esta almacenada de manera electrónica. Existe poca documentación en papel que soporta la información corporativa.

Gestión de la Información. Uno de los objetivos del Departamento de Tecnología de la CORPAIRE es gestionar la información de la misma. Este departamento es el responsable de realizar la correcta Gestión de la Información.

Acceso a la Información. El Departamento de Tecnología de la CORPAIRE es el responsable de autorizar o negar el acceso a la información.

1.2.2 PUNTO DE VISTA NORMATIVO – LEGAL

El Municipio del Distrito Metropolitano de Quito y el Consejo Nacional de Tránsito crearon la Corporación Centros de Revisión y Control Vehicular, como una persona jurídica de derecho privado sin fines de lucro, la misma que fue reconocida mediante Acuerdo Ministerial de Gobierno número 289 de 7 de agosto de 2001. Posteriormente se integraron a su Directorio, la Comandancia General de la Policía Nacional, la Dirección Metropolitana de Medio Ambiente de Quito, la Dirección Nacional de Tránsito, la Escuela Politécnica Nacional y Fundación Natura.

Por resolución del Directorio de la Corporación, ésta se hizo cargo del manejo de la Red de monitoreo Atmosférico de Quito (UREMAQ), con lo cual modificó su nombre y su estatuto ante la misma Cartera de Estado, la que reconoció a CORPAIRE, Corporación para el Mejoramiento del Aire de Quito, mediante Acuerdo 004 de 18 de febrero de 2004.

El 16 de octubre de 2009, el Acta de la Asamblea de la Corporación para el Mejoramiento del Aire de Quito - CORPAIRE, dentro de las consideraciones para la disolución de la Corporación, contempla el alinear el accionar del municipio al nuevo marco constitucional. Entre otras resoluciones dispuestas es: el mantener las operaciones de la Corporación hasta la culminación del proceso de disolución y liquidación, siempre que éstas no puedan ser trasladadas a un órgano o entidad municipal, sin afectar la continuidad del servicio a la comunidad.

Toda esta base legal que rige a la CORPAIRE evidencia la necesidad de elaborar Políticas de Seguridad de la Información que permitan garantizar la integridad, confidencialidad y disponibilidad de la información.

1.2.3 PUNTO DE VISTA CORPORATIVO

El apoyo de las autoridades de la CORPAIRE para la implementación de las Políticas de Seguridad de la Información es de vital importancia, los directivos deben tomar en cuenta la importancia de la aplicación de las políticas y su alineación de estas a las necesidades y objetivos estratégicos de la corporación.

Para tener un apoyo total de las autoridades las políticas deben ser elaboradas en función de las necesidades de la corporación. En tal virtud, es necesario conocer la estructura organizacional de la corporación.

1.3 ORGANIZACIÓN DE LA CORPORACIÓN

La CORPAIRE, Corporación Municipal para el mejoramiento del Aire de Quito, nació en febrero del 2004 mediante un Acuerdo del Ministerio de Gobierno, a partir de una innovadora propuesta del Municipio del Distrito Metropolitano de Quito para consolidar una estructura institucional que posibilite una gestión adecuada de la calidad del aire.

Los antecedentes inmediatos son la vigencia del proceso obligatorio de Revisión Técnica Vehicular (RTV), manejado originalmente por la Corporación Centros de Revisión Vehicular, y la puesta en marcha de la Red Metropolitana de Monitoreo Atmosférico de Quito, operada en su primer año por la Empresa de Desarrollo del Centro Histórico.

Misión

Mejorar la calidad del aire de Quito, a través de una gestión basada en sólidos conocimientos científicos, en la participación ciudadana y los consensos institucionales.

Visión

Institución consolidada dentro del esquema de gobierno local, constituida en referente nacional e internacional por su transparencia y efectividad en la ejecución de programas relevantes para el mejoramiento de la calidad del aire del Distrito Metropolitano de Quito.

Organigrama Funcional

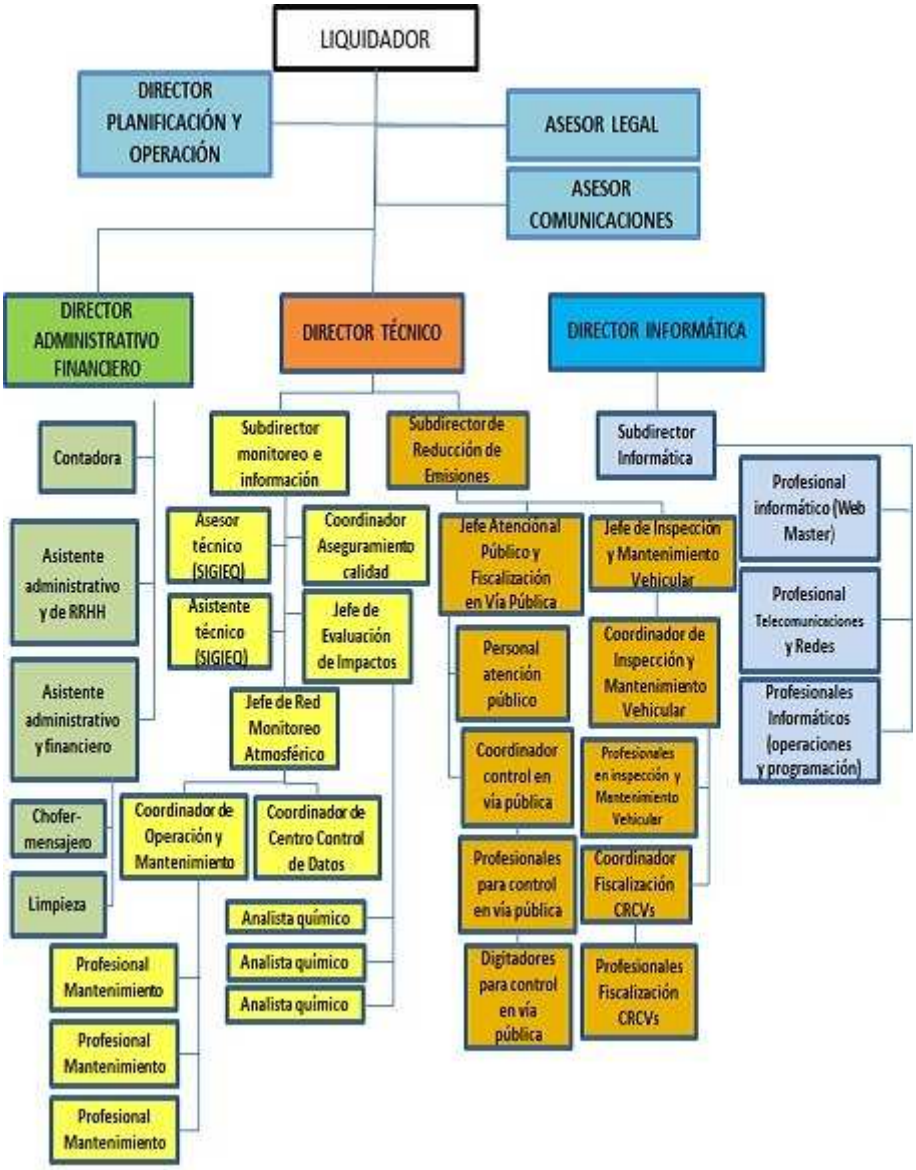

Figura 1.1 Organigrama Funcional de la CORPAIRE

1.3.1 EL ACCIONAR DE LA CORPAIRE

El manejo presupuestario es auditado anualmente por una empresa independiente y la gestión administrativa es evaluada por la Dirección General de Auditoría Interna del Municipio del Distrito Metropolitano de Quito. Los informes son conocidos y discutidos por el Directorio y pueden ser revisados, junto con el resto de la información institucional, en el sitio Web de la CORPAIRE, de acuerdo con las disposiciones de la Ley Orgánica de Transparencia y Acceso Público a la Información (LOTAIP).

El eje de la acción de la CORPAIRE constituye el Plan de Manejo de la Calidad del Aire del Distrito Metropolitano de Quito 2005-2010 (PMCA-Q), aprobado por el Concejo Metropolitano en agosto del 2005. Este instrumento se enmarca en los lineamientos generales del Plan Maestro de Gestión Ambiental y la visión estratégica de desarrollo del Distrito Metropolitano de Quito plasmada en el Plan Equinoccio 21, que plantea la sostenibilidad ambiental como la base para el equitativo, solidario y sostenido mejoramiento de la calidad de vida de los habitantes de Quito.

El PMCA-Q busca prevenir y evitar los daños a la salud humana, a los recursos naturales y al patrimonio cultural, derivados de la calidad del aire, a través de un conocimiento objetivo de la realidad local y las mejores experiencias internacionales, y la aplicación efectiva y eficiente de las medidas políticas, técnicas y económicas más apropiadas. Adicionalmente el Plan considera esfuerzos orientados a minimizar las emisiones de gases de efecto invernadero, causantes del cambio climático global.

1.3.2 DIRECTORIO DE LA CORPAIRE

Dr. Augusto Barrera
Alcalde Metropolitano de Quito

Señor General de Distrito Freddy Martínez Pico
Comandante General de la Policía Nacional

Señor Ramiro Morejón
Secretario de Ambiente (e)

Ingeniero Fernando Amador
Subsecretario de Transportes Presidente del Consejo Nacional de Tránsito, Transporte Terrestre y Seguridad Vial

Coronel de Policía Pedro Calero
Dirección Nacional de Tránsito

Xavier Bustamante P.
Director Ejecutivo Fundación Natura

Ingeniero Alfonso Espinosa Ramón
Rector de la Escuela Politécnica Nacional

1.4 DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA CORPAIRE

CORPAIRE cuenta con un sistema informático centralizado y transaccional, que en un solo entorno resuelve la mayoría de los procesos que se incluyen en el manejo de la abundante información relacionada con la RTV, de modo que se logra brindar un apropiado servicio a los ciudadanos del Distrito Metropolitano.

Por su compleja naturaleza y la imperiosa necesidad de que este sistema brinde todos sus servicios en forma ininterrumpida, se estructuró un entorno tecnológico seguro, de alta confiabilidad y alta disponibilidad.

Se cuenta con una extensa red privada de telecomunicaciones con tecnologías de microondas y con los anchos de banda requeridos para satisfacer la alta

transaccionalidad existente, de manera ágil, sin retardos, ni limitaciones de ninguna especie.

CORPAIRE, además de tener unas de las más modernas estructuras tecnológicas, cuenta con una actualizada red de computadores personales, una central telefónica digital, teléfonos y faxes digitales, red de impresoras, copiadoras y toda una gama de recursos tecnológicos que permiten un correcto y eficiente desempeño de las funciones de todo el personal de la organización.

1.4.1 MISIÓN

Gestionar de la manera más eficiente, correcta y oportuna toda la infraestructura tecnológica de la CORPAIRE para satisfacer las necesidades de todos los usuarios, todo esto alineado a los objetivos estratégicos de la corporación.

1.4.2 VISIÓN

Ser un departamento que además de brindar un servicio de calidad, genere valor agregado en cada una de las actividades que realiza la corporación.

1.4.3 OBJETIVOS

- Administrar el Sistema Centralizado de Revisión Técnica Vehicular (SC-RTV)
- Brindar soporte a usuarios en los recursos informáticos
- Desarrollar y mantener el SC-RTV
- Coordinar actividades informáticas con los Centros de Revisión y Control Vehicular.
- Brindar asesoría en la adquisición de recursos informáticos a los directivos de la corporación.

- Presentar proyectos de actualización y renovación de los sistemas informáticos, en función de los avances tecnológicos y las necesidades de la corporación.
- Gestionar la información de todos los activos de información que tiene la corporación.
- Centralizar toda la información de la CORPAIRE.
- Proporcionar información gerencial de manera oportuna como apoyo para la toma de decisiones.
- Elaborar el plan estratégico anual.
- Implementar y gestionar controles, políticas, procesos y procedimientos para el correcto funcionamiento de los recursos informáticos.

1.4.4 ORGANIGRAMA

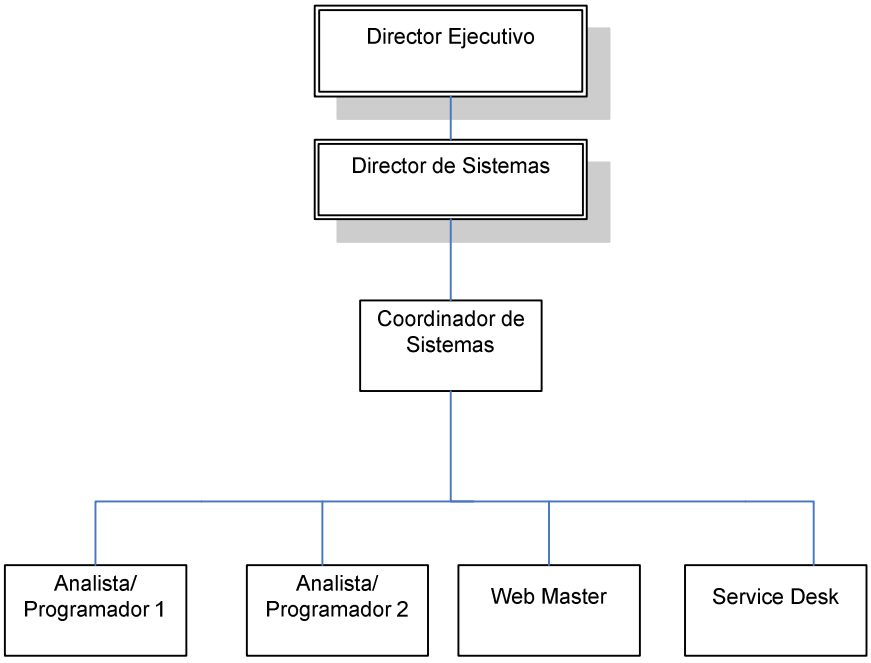

Figura 1.2 Organigrama del Departamento de Tecnología

1.4.5 ESQUEMA DE RED ACTUAL DE LA CORPAIRE

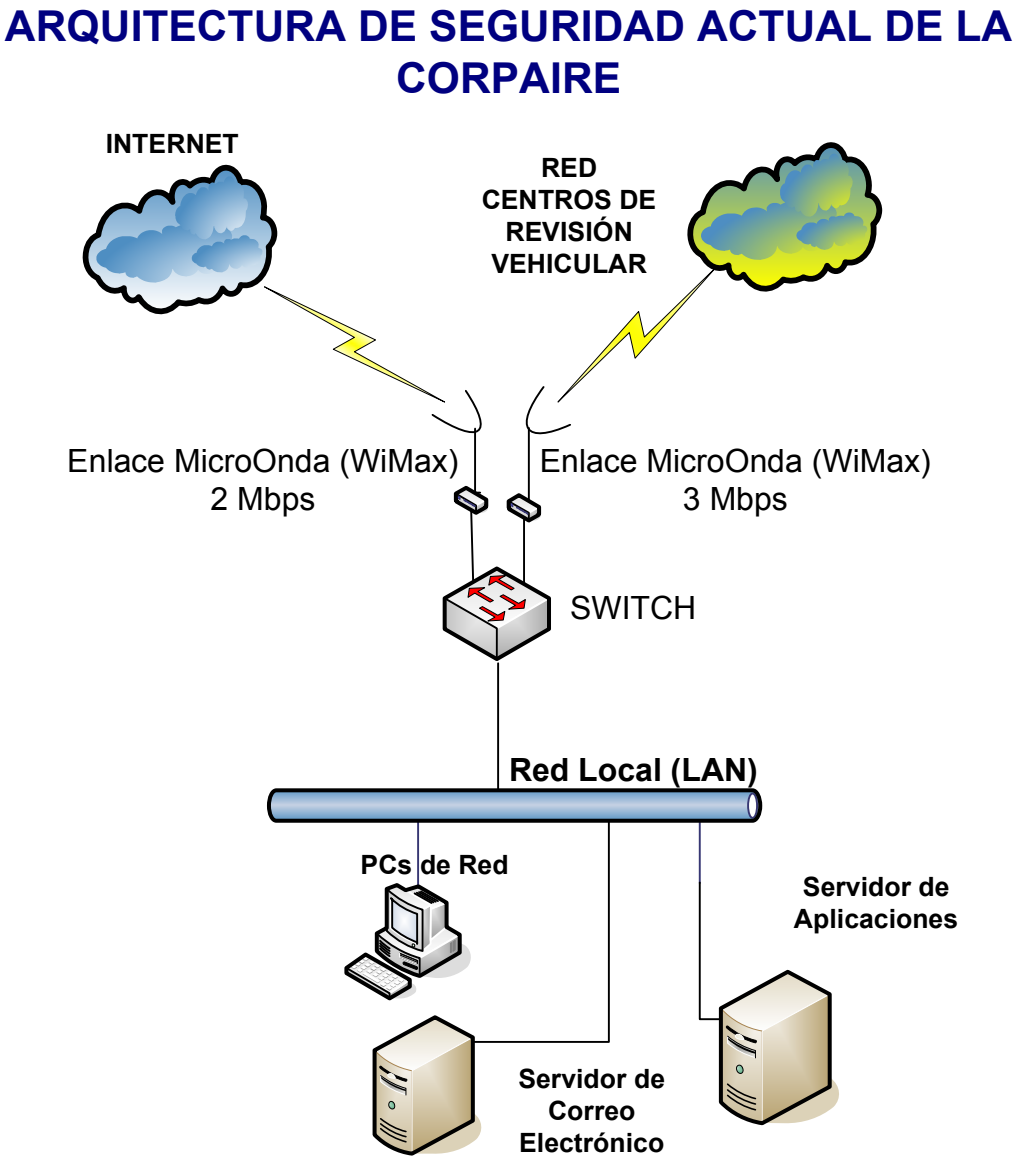

Figura 1.3 Esquema de Seguridad Actual de la CORPAIRE

CAPÍTULO 2

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

2.1 ANÁLISIS DE LOS MARCOS DE TRABAJO

En la actualidad, dada las condiciones sobre las que se desarrollan las Tecnologías de la Información, existen una variedad de marcos de trabajo para el Análisis y Evaluación de Riesgos de Seguridad de la Información, que se usan como referencia para enfrentar y resolver nuevos problemas de índole similar.

En el plan de tesis presentado y aprobado para el desarrollo de este proyecto, dentro de la justificación metodológica se menciona el uso de la Norma ISO 27005:2008 para la Evaluación del Riesgo, sin embargo es necesario citar adicionalmente dos marcos de trabajo para comparar y justificar su uso.

2.1.1 ISO/IEC 27005:2008 GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Publicada el 4 de junio de 2008. Establece las directrices para la Gestión del Riesgo en la Seguridad de la Información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. [2]

El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 es importante para un completo entendimiento de la norma ISO/IEC 27005:2008 que es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que tienen la intención de gestionar los riesgos que puedan comprometer la seguridad de la información

[2] Tomado de: La página web de la Norma ISO www.iso.org

de la organización. Su publicación revisa y retira las normas ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335:2000.

Esta norma considera análisis cualitativos y cuantitativos. En la actualidad se concentra en la evaluación del riesgo y su tratamiento. La ISO/IEC 27005 contiene numerosos anexos útiles como: valoración del activo, evaluación del impacto, ejemplo de listas de amenazas, ejemplo de listas de vulnerabilidades relacionadas con áreas específicas de seguridad de la información, análisis de varios enfoques de evaluación del riesgo y mucha información acerca de la selección de controles (con base en la antigua ISO/IEC 13335-4).

Este estándar proporciona una lista de dominios de riesgo que deben ser considerados, los cuales son: Aplicaciones, Información, Servicios, Procesos empresariales, Entorno Físico, Personas, Tecnologías de la Información, y Conexiones en Red.

El proceso de gestión de riesgos de la norma ISO 27005:2008 se describe en las siguientes 6 cláusulas:

Cláusula 7 Establecimiento del contexto, en la que se define los objetivos, el alcance y la organización para todo el proceso.

Cláusula 8 Valoración del Riesgo, en la que se obtiene toda la información necesaria para conocer, valorar y priorizar los riesgos. Se divide en tres apartados:

- Identificación del riesgo, que consiste en determinar qué puede provocar pérdidas a la organización.
- Análisis del riesgo, que consiste en utilizar métodos cuantitativos o cualitativos para obtener una cuantificación de los riesgos identificados, tomando en cuenta los activos, las amenazas y las políticas.
- Evaluación del riesgo, consiste en comparar los riesgos estimados con los criterios de evaluación y de aceptación de riesgos definidos en el establecimiento del contexto.

Cláusula 9 Tratamiento del Riesgo, en esta se define la estrategia para tratar cada uno de los riesgos valorados: reducción, aceptación, evitación o transferencia.

Cláusula 10 Aceptación del Riesgo, en la que se determina los riesgos que se decide aceptar y la justificación correspondiente a cada riesgo aceptado.

Cláusula 11 Comunicación del Riesgo, en esta todos los grupos de interés intercambian información sobre los riesgos.

Cláusula 12 Monitorización y Revisión del Riesgo, en la que el análisis de riesgos se actualiza con todos los cambios internos o externos que afectan la valoración de los riesgos.

El proceso de Gestión de Riesgos definido en la Norma ISO/IEC 27005:2008 puede resumirse en la figura 2.1.

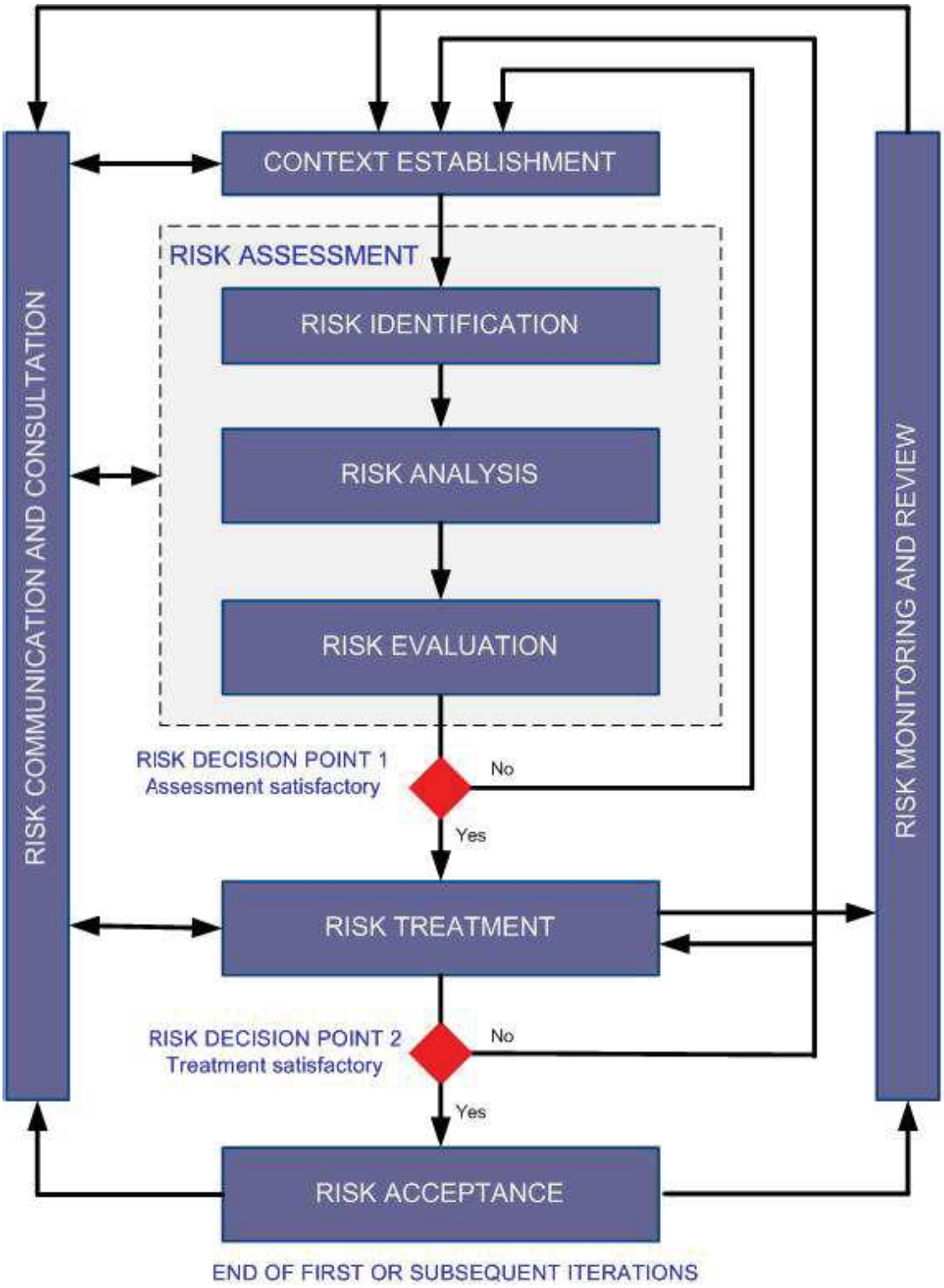

Figura 2.1 Proceso de Gestión de Riesgos ISO 27005:2008

En línea con el estándar ISO/IEC 27001:2005, el proceso de Gestión de Riesgos se considera iterativo siguiendo el ciclo de Deming. Eso se describe en la figura 2.2 y en la tabla 2.1.

Figura 2.2 Ciclo de Deming

Fuente: http://www.terra.es/personal3/lilelile/

Ciclo de Deming	Proceso de Gestión de Riesgos de Seguridad de la Información
Planificar (P)	Establecimiento del contexto Valoración del riesgo Desarrollo del plan de tratamiento del riesgo Aceptación del riesgo
Hacer (D)	Implantación de plan de tratamiento del riesgo
Verificar (C)	Monitorización y revisión contínua del riesgo
Actuar (A)	Mantenimiento y mejora del proceso de Gestión de Riesgos de Seguridad de la Información

Tabla 2.1 Ciclo de Deming para la ISO/IEC 27005:2008

Como resumen de este estándar se presenta un listado de las principales ventajas y desventajas. Tal como se muestra en la tabla 2.2.

VENTAJAS
Es un complemento de la ISO 27001 y la ISO 27002.
Es un estándar internacional, lo que le faculta mayor aceptación.
Publicación reciente de su última versión es 2008.
Posee una cláusula completa orientada a la monitorización y revisión de riesgos.
Se la considera con un alcance completo, tanto en el análisis como en la gestión de riesgos.
Posee la fase de aceptación de riesgos, previa su justificación.
Permite un análisis completo cuantitativo.
DESVENTAJAS
No es certificable
No posee herramientas, técnicas, ni comparativas de ayuda para su implementación.

Tabla 2.2 Ventajas y Desventajas de la ISO/IEC 27005:2008

2.1.2 NIST 800-30: RISK MANAGEMENT GUIDE FOR INFORMATION TECHNOLOGY SYSTEMS.

El NIST (National Institute of Standards and Technology) de los Estados Unidos, fue fundado en 1901 y es un referente a nivel mundial dentro del campo de la investigación y estandarización de actividades técnicas, tanto dentro como fuera de Norteamérica.

El NIST propone varios documentos contenidos en una Guía de Documentos con información detallada acerca de los procedimientos técnicos que deberían ser adoptados para garantizar un alto nivel de desempeño y disponibilidad de muchos servicios dentro de una institución. En varios de estos estándares se documentan las mejores prácticas organizacionales que podrían ser utilizadas para la creación de políticas y procedimientos en el área informática de una organización.

NIST 800-30: Risk Management Guide for Information Technology Systems.

El riesgo es el impacto negativo del ejercicio de una vulnerabilidad, considerando tanto la probabilidad así como el impacto de la ocurrencia. La administración de los riesgos es el proceso de identificar los riesgos, evaluación de riesgos y toma de decisiones para reducir el riesgo a un nivel aceptable.

Esta guía provee fundamentos para el desarrollo de un programa de administración de riesgos efectivo, conteniendo tanto las definiciones como una guía práctica necesaria para la evaluación y mitigación de riesgos identificados dentro de los sistemas de Tecnologías de la Información. El objetivo primordial es ayudar a las organizaciones a una mejor administración o manejo de los riesgos relacionados con la misión de las Tecnologías de la Información.

Esta guía contempla lo siguiente:

1. Introducción
2. Panorama de la Administración de Riesgos
3. Evaluación de Riesgos
4. Mitigación de Riesgos
5. Análisis y Evaluación

Como resumen de esta metodología se presenta un listado de las principales ventajas y desventajas. Tal como se muestra en la tabla 2.3.

VENTAJAS
Provee fundamentos para el desarrollo de un programa de administración de riesgos efectivo.
Ayuda a las organizaciones a una mejor administración de los riesgos.
Posee una cláusula completa orientada a la monitorización y revisión de riesgos.
Pertenece a NIST, Instituto de Estándares líder en los Estados Unidos.
Permite un análisis cuantitativo.

DESVENTAJAS
No permite un análisis cualitativo.
No involucra a los procesos como elementos del modelo a seguir.
No posee herramientas, técnicas, ni comparativas de ayuda para su implementación.

Tabla 2.3 Ventajas y Desventajas de NIST 800-30

2.1.3 MAGERIT: METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE LA INFORMACIÓN.

La metodología MAGERIT fue desarrollada por el Consejo Superior de Administración Electrónica de España. El Consejo Superior de Administración Electrónica es el órgano colegiado adscrito al Ministerio de Administraciones Públicas, encargado de la preparación, elaboración, desarrollo y aplicación de la política y estrategia del Gobierno en materia de Tecnologías de la Información, así como del impulso e implantación de la Administración Electrónica en la Administración General del Estado.

La primera versión se publicó en 1997 y en la actualidad la versión 2.0 es la vigente, publicada en 2006.

Se trata de una metodología abierta, de uso muy extendido en el ámbito español, y de uso obligatorio por parte de la Administración Pública de Española. Dispone de una herramienta de soporte, PILAR II (Proceso Informático Lógico para el Análisis y la Gestión de Riesgos), de uso gratuito para la Administración Pública española y con costo para organizaciones privadas.

La metodología consta de tres volúmenes:

Volumen I – Método, es el volumen principal en el que se explica detalladamente la metodología.

Volumen II – Catálogo de elementos, proporciona diversos inventarios de utilidad en la aplicación de la metodología. Los inventarios que incluye son:

- Dimensiones y criterios de valoración
- Amenazas
- Tipos de Activos
- Tipos de Recursos de Información
- Políticas

Volumen III – Guía de Técnicas, proporciona una introducción de algunas técnicas a utilizar en las distintas fases del análisis de riesgos. Las técnicas que recoge son:

- Técnicas especificas para el análisis de riesgos:
  - Análisis mediante tablas
  - Análisis algorítmico
  - Árboles de ataque
- Técnicas generales
  - Análisis costo-beneficio
  - Diagramas de Flujo de Datos (DFD)
  - Diagramas de procesos
  - Técnicas gráficas
  - Planificación de Proyectos
  - Sesiones de Trabajo: entrevistas, reuniones y presentaciones
  - Valoración Delphi

Como resumen de esta metodología se presenta un listado de las principales ventajas y desventajas. Tal como se muestra en la tabla 2.4.

VENTAJAS
Se la considera con un alcance completo, tanto en el análisis como en la gestión de riesgos.
Posee un extenso archivo de inventarios en lo referente a Recursos de Información, Amenazas y Tipo de Activos
Permite un análisis completo cualitativo y cuantitativo

Dispone de una herramienta de soporte PILAR II
Es una metodología líder en España, con buenos referentes de aplicación.
DESVENTAJAS
No involucra a los procesos, recursos ni vulnerabilidades como elementos del modelo a seguir.
No posee un inventario completo en lo referente a Políticas.
No es una metodología reconocida en el Ecuador.

Tabla 2.4 Ventajas y Desventajas de MAGERIT

2.2 SELECCIÓN DEL MARCO DE TRABAJO A UTILIZAR

2.2.1 SELECCIÓN DEL MARCO DE TRABAJO A UTILIZAR

Luego de citar los marcos de trabajo para el análisis y evaluación de riesgos, se realiza la selección en base a parámetros que son necesarios y que deben cumplir la metodología a utilizar.

A continuación se describen cinco parámetros o factores determinantes para la selección del marco de trabajo a utilizar.

1. **Valoración del Riesgo**. Para identificar los riesgos existentes, el marco de trabajo debe considerar las siguientes actividades:
    a) Identificación de Activos
    b) Identificación de Amenazas
    c) Identificación de Existencia de Controles
    d) Identificación de Vulnerabilidades
2. **Análisis Cualitativo y Cuantitativo**. Luego de identificar los riesgos, el marco de trabajo debe considerar una metodología de análisis de riesgo. El análisis de riesgo cualitativo usa una escala de calificación de atributos para describir la magnitud de las consecuencias potenciales (por ejemplo baja, media y alta) y la probabilidad de esas consecuencias. En este proyecto de tesis se utilizará el método cualitativo.
3. **Evaluación del Riesgo**. El marco de trabajo debe considerar los siguientes aspectos:

a) Criterios de evaluación del riesgo
b) Criterios de Impacto

4. **Elementos de Modelo.** El marco de trabajo debe proporcionar una lista de dominios de riesgo que deben ser considerados, los cuales son:
   a) Organización
   b) Procesos y procedimientos
   c) Personal
   d) Operaciones diarias
   e) Ambiente Físico
   f) Hardware, Software, Comunicaciones
   g) Dependencias Externas
5. **Anexos con ejemplos**. Debe poseer información adicional para las actividades de Gestión de Riesgos de Seguridad de la Información. Por ejemplo anexos como: valoración del activo, evaluación del impacto, ejemplo de listas de amenazas, ejemplo de listas de vulnerabilidades relacionadas con áreas específicas de seguridad de la información, análisis de varios enfoques de evaluación del riesgo, etc.

Cada parámetro tiene un peso (valor ponderado) y que es igual a la suma de sus variables. Ejemplo:

		Valor Ponderado
Parámetro:	3. Evaluación del Riesgo	0.10
Variables:	a) Criterios de Evaluación del Riesgo	0.05
	b) Criterios de Impacto	0.05

Entonces, los valores ponderados de cada parámetro son:

1.	Valoración del riesgo	0.40
2.	Análisis Cualitativo y Cuantitativo	0.10
3.	Evaluación del Riesgo	0.40
4.	Elementos de Modelo	0.07
5.	Anexos con ejemplos	0.03

Estos valores están dados en función de la importancia que representa el parámetro en el marco de trabajo para realizar el Análisis y Evaluación de

Riesgos. Para obtener la valoración de cada parámetro se califica con un valor de 1 a 10 a cada variable. Para un mejor entendimiento se visualiza la tabla 2.5 con el análisis de comparación de los tres marcos de referencia.

ANÁLISIS DE COMPARACIÓN

	FACTORES DETERMINANTES	PESO	ISO 27005:2008		NIST 800-30		MAGERIT	
			Calific	Valor	Calific	Valor	Calific	Valor
1	**Valoración del Riesgo**	**0.40**	**10**	**4**	**10**	**4**	**7.5**	**3**
	a) Identificación de Activos	0.10	10	1	10	1	10	1
	b) Identificación de Amenazas	0.10	10	1	10	1	10	1
	c) Identificación de Existencias de Controles	0.10	10	1	10	1	10	1
	d) Identificación de Vulnerabilidades	0.10	10	1	10	1	0	0
2	**Análisis Cualitativo y Cuantitativo**	**0.10**	**10**	**1**	**5**	**0.5**	**10**	**1**
	a) Cualitativo	0.05	10	0.5	0	0	10	0.5
	b) Cuantitativo	0.05	10	0.5	10	0.5	10	0.5
3	**Evaluación del Riesgo**	**0.40**	**10**	**4**	**7**	**2.8**	**8**	**3.2**
	a) Criterios de Evaluación del Riesgo	0.20	10	2	10	2	10	2
	b) Criterios de Impacto	0.20	10	2	4	0.8	6	1.2
4	**Elementos de Modelo**	**0.07**	**10**	**0.7**	**8.6**	**0.6**	**8.57143**	**0.6**
	a) Organización	0.01	10	0.1	10	0.1	10	0.1
	b) Procesos y procedimientos	0.01	10	0.1	0	0	0	0
	c) Personal	0.01	10	0.1	10	0.1	10	0.1
	d) Operaciones diarias	0.01	10	0.1	10	0.1	10	0.1
	e) Ambiente Físico	0.01	10	0.1	10	0.1	10	0.1
	f) Hardware, Software, Comunicaciones	0.01	10	0.1	10	0.1	10	0.1
	g) Dependencias Externas	0.01	10	0.1	10	0.1	10	0.1
5	**Anexos con ejemplos**	**0.03**	**10**	**0.3**	**1**	**0.03**	**0.5**	**0.02**
	Total	**1.00**		**10.0**		**7.9**		**7.8**

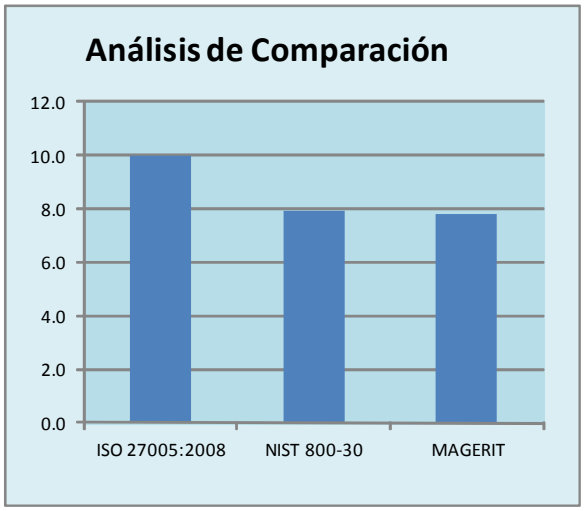

Tabla 2.5 Análisis de Comparación de Marcos de Trabajo

Del análisis de comparación de los tres marcos de trabajo, se puede notar que la Norma ISO/IEC 27005:2008 cumple con todos los parámetros determinantes para realizar el análisis y evaluación de riesgos de seguridad de la Información.

Además de tomar en cuenta el análisis de los marcos de trabajo, también se considera que la Norma ISO/IEC 27005:2008 es aplicable a todo tipo de organización y su modelo de metodología se ajusta a las necesidades de la institución.

2.2.2 DESCRIPCIÓN DE LA NORMA ISO/IEC 27005:2008

2.2.2.1 ESTRUCTURA DEL ESTANDARD

Esta norma contiene la descripción del proceso de Gestión de Riesgos de Seguridad de la Información y sus actividades.

La información adicional de la gestión de riesgos de seguridad de la información se presenta en anexos de esta norma. El establecimiento del contexto es apoyado por el Anexo A (**Definiendo el alcance y los límites del proceso de gestión de riesgos de seguridad de la información**). La identificación y valoración de los activos y evaluaciones del impacto se analizan en el Anexo B (**Ejemplos de identificación de activos**), en el Anexo C (**Ejemplos de amenazas típicas**) y en el Anexo D (**Vulnerabilidades y métodos para la evaluación de la vulnerabilidad**). Ejemplos de evaluación de riesgos de seguridad de la información se presentan en el Anexo E. Las limitaciones para reducir el riesgo se presentan en el Anexo F.[3]

Todas las actividades de la gestión de riesgos desde la Cláusula 7 a la Cláusula 12 están estructuradas de la siguiente forma:

Entrada: Identifica cualquier información necesaria para realizar la actividad.
Acción: Describe la actividad.

[3] Tomado de: ISO-IECJTC1-SC27_N8923_FCD_27005_20100602

Guía de Implementación: Ofrece orientación sobre cómo efectuar la acción. Algunas de estas orientaciones puedes no ser adecuadas en todos los casos y de ese modo otras formas de realizar la acción pueden ser más apropiadas.
Salida: Identifica cualquier información obtenida tras realizar la actividad.

A continuación se describe brevemente cada una de las seis cláusulas que enmarcan todo el proceso de Gestión de Riesgos de Seguridad de la Información de la Norma ISO/IEC 27005:2008.

2.2.2.2 CLÁUSULA 7 ESTABLECIMIENTO DEL CONTEXTO

Entrada: Toda la información sobre la organización referente al contexto de gestión de riesgos de seguridad de la información.

Acción: El contexto externo e interno para la gestión de riesgos de seguridad de la información debe ser establecido, este implica el ajuste de los criterios básicos necesarios para la gestión de riesgos de seguridad de la información, definiendo los alcances y términos; y el establecimiento de una organización apropiada que maneje la gestión de riesgos de seguridad de la información.

Guía de Implementación: Esta guía esencialmente determina el objetivo de la gestión de riesgos de seguridad de la información, como esto afecta a todos los procesos y al establecimiento del contexto en particular.

Salida: Las especificaciones de los criterios básicos, el alcance y límites; y la organización de la información para el proceso de gestión de riesgos de seguridad de la información.

2.2.2.3 CLÁUSULA 8 VALORACIÓN DEL RIESGO

Entrada: Criterios básicos, el alcance y los límites; y la organización para el proceso de riesgos de seguridad de la información establecido.

Acción: Los riesgos deben ser identificados, descritos cuantitativamente o cualitativamente; y priorizados entre los criterios de la evaluación del riesgo y los objetivos relevantes de la organización.

Guía de Implementación: Un riesgo es una combinación de las consecuencias que se darían a la presencia de un evento no deseado y la probabilidad de la ocurrencia del evento. La evaluación del riesgo describe cuantitativamente o cualitativamente el riesgo y permite gestionar la prioridad de los riesgos de acuerdo a la seriedad percibida u otros criterios establecidos.

La valoración del riesgo consiste de las siguientes actividades:

- Identificación del Riesgo
- Análisis de Riesgo
- Evaluación del Riesgo

Salida: Una lista de valoración de riesgos priorizados de acuerdo a lo criterios de evaluación del riesgo.

2.2.2.4 CLÁUSULA 9 TRATAMIENTO DEL RIESGO

Entrada: Una lista de prioridades de los riesgos según los criterios de evaluación del riesgo en relación con los escenarios de incidentes que conducen a esos riesgos.

Acción: Controles para reducir, conservar, evitar, o compartir los riesgos deben ser seleccionados y definidos en un plan de tratamiento del riesgo.

Guía de Implementación: Hay cuatro opciones disponibles para el tratamiento de riesgos: reducción del riesgo, retención del riesgo, evitar el riesgo y compartir el riesgo.

Salida: Plan de tratamiento del riesgo y riesgos residuales sujetos a la aceptación de una decisión de los directivos de la organización.

2.2.2.5 CLÁUSULA 10 ACEPTACIÓN DEL RIESGO

Entrada: El plan de tratamiento de riesgo y la evaluación de riesgo residual están sujetos a la decisión acertada de directivos de la organización.
Acción: La decisión de aceptar los riesgos y responsabilidades debe hacerse y registrarse formalmente.

Guía de Implementación: Los planes de tratamiento del riesgo deberán describir cuan evaluados están los riesgos a ser tratados, para satisfacer los criterios de aceptación del riesgo. Es importante que los gerentes responsables revisen y aprueben las propuestas de planes de tratamiento del riesgo y por consiguiente el riesgo residual, y registren las condiciones asociadas con dicha autorización.
Salida: Una lista de riesgos aceptados con justificación para aquellos que no cumplan los criterios de aceptación normal del riesgo de la organización.

2.2.2.6 CLÁUSULA 11 COMUNICACIÓN DEL RIESGO

Entrada: Toda la información de riesgos obtenida de la gestión de riesgos.

Acción: La información acerca del riesgo debe ser intercambiada y/o compartida entre el tomador de decisiones y los accionistas.

Guía de Implementación: La comunicación del riesgo es una actividad para lograr un acuerdo sobre cómo gestionar los riesgos mediante el intercambio y/o el compartir información acerca del riesgo entre los que toman las decisiones y los accionistas. La información incluye, pero no se limita a la existencia de los riesgos de la naturaleza, forma, probabilidad, gravedad, tratamiento y aceptabilidad.

Salida: La continua comprensión de los procesos y resultados de la gestión de riesgos de seguridad de la información de la organización.

2.2.2.7 CLÁUSULA 12 MONITORIZACIÓN Y REVISIÓN DEL RIESGO

Entrada: Toda la información de los riesgos obtenida de la gestión de riesgos.

Acción: Los riesgos y sus factores (es decir valor de activos, impactos, amenazas, vulnerabilidades, y la probabilidad de ocurrencia) deben ser supervisados y examinados para determinar los cambios en el contexto de la organización en una etapa temprana, y mantener un panorama general de la fotografía completa del riesgo.

Guía de Implementación: Los riesgos no son estáticos. Las amenazas, vulnerabilidades, la probabilidad o las consecuencias pueden cambiar repentinamente sin ninguna indicación. Por lo tanto es necesaria una vigilancia constante para detectar estos cambios. Esto puede ser apoyado por servicios externos que proporcionan información sobre las nuevas amenazas o vulnerabilidades.

Salida: Una continua alineación de la gestión de riesgos con los objetivos empresariales de la organización y con los criterios de aceptación del riesgo.

2.3 VALORACIÓN Y EVALUACIÓN DEL RIESGO

La importancia del Análisis de Riesgos deriva en que es la herramienta que permite:

- Identificar las amenazas a las que se encuentran expuestos los activos de información.
- Estimar la frecuencia de materialización de tales amenazas.
- Valorar el impacto que supondría para la organización esa materialización.

La ISO/IEC 27005:2008 proporciona un conjunto de directrices para la correcta realización de un Análisis de Riesgos. No obstante esta norma no proporciona una metodología concreta de Análisis de Riesgos, sino que describe a través de su clausulado el proceso recomendado de análisis.

La norma sirve para no tener dudas sobre los elementos que debe incluir toda buena metodología de Análisis de Riesgos, por lo que, visto desde este punto de vista puede constituirse como una metodología misma.

El estándar incluye seis anexos (A-F) de carácter informativo y no normativo, con orientaciones que van desde la identificación de activos e impactos, ejemplos de vulnerabilidades y sus amenazas asociadas, hasta distintas aproximaciones para el análisis distinguiendo entre análisis de riesgo de alto nivel y análisis detallado.

Como el alcance de este proyecto de tesis consiste en una Propuesta de Políticas de Seguridad de la Información y su paso previo es realizar una Valoración y Evaluación de Riesgos de Seguridad de la Información de los activos de información de la CORPAIRE, solamente se usará la cláusula 8 Valoración del Riesgo para realizar dicho proceso.

2.3.1 VALORACIÓN DEL RIESGO

2.3.1.1 Identificación del Riesgo

2.3.1.1.1 Identificación de Activos

Para llevar a cabo la valoración de activos, la corporación necesita primero identificar sus activos (a un nivel adecuado de detalle). Para aquello los activos se han divido en dos clases:

Activos Primarios:

- Procesos y actividades de negocio
- Información

Activos de Apoyo:

- Hardware
- Software
- Red
- Recurso Humano

En base a estas dos clases de activos, los activos de información de la CORPAIRE se visualizan en la tabla 2.6.

TIPO	ACTIVOS DE INFORMACIÓN
Procesos y actividades del negocio	Revisión Técnica Vehicular(RTV)
	Monitoreo de la Calidad del Aire
	Fiscalización de los centros de revisión
	Control en vía pública
	Atención al Cliente
Información	Bases de Datos del Sistema Centralizado de Revisión Técnica Vehicular (SC-RTV)
	Archivos de trabajo de funcionarios
	Manuales de Control de Calidad
	Bases de Datos de Correo Electrónico
	Instructivos de Revisión Técnica Vehicular
Hardware	Servidores Iseries
	Unidades de expansión
	Servidor de Virtualización
	Servidor de Correo
	Servidor de Internet
	Computadores Personales
	Computadores Portátiles
	Central Telefónica
	PDAs
	Impresoras
	Teléfonos terminales
	Fax
	Cintas de Backup
	Discos Duros removibles
	Proyectores
Software	Sistema Operativo OS/400
	Sistema Centralizado de Revisión Técnica Vehicular (SC-RTV)
	Lotus Notes
	Client Access
	Microsoft Office
	Windows XP
	Linux
	Gestión de Central Telefónica
Red	Ruteadores
	Switches
	Radio enlaces
	Red de Area Local
Recurso Humano	Dirección General
	Recursos Humanos
	Dirección Financiera
	Adminstrador del Sistema
	Grupo de Desarrollo de Sistemas

Tabla 2.6 Activos de Información de la CORPAIRE

2.3.1.1.2 Identificación de Amenazas

El objetivo es identificar las amenazas a las que están expuestos los activos de información. Una amenaza puede ser de origen Natural o Ambiental, Humana o Accidentales, Técnica, y Organizacional. A continuación se detalla en la tabla 2.7 a las posibles amenazas agrupadas por su origen.

Amenazas Naturales o Ambientales	
FUENTE DE AMENAZA	**ACCIONES DE LA AMENAZA**
Sismo	Destrucción de infraestructura física. Daño al personal.
Tormenta Eléctrica	Falla eléctrica (suspensión de servicio eléctrico) Daño de equipos
Falla Eléctrica	Servicios no disponibles. Fallo integral de la información. Desconfiguración de aplicaciones y servicios. Daño de equipos.
Polución	Daño de equipos. Problemas de salud en las personas.
Humedad/Corrosión	Daño de equipos. Incomodidad para las personas en el desarrollo de sus actividades.
Animales (roedores, insectos, etc.)	Daños en equipos.
Condiciones de trabajo inadecuadas	Problemas ergonómicos. Disminución de eficiencia del personal. Pérdida de la concentración. Malestar en el personal.
Amenazas Humanas o Accidentales	
FUENTE DE AMENAZA	**ACCIONES DE LA AMENAZA**
Pérdida de personal	Disponibilidad de personal. Suspensión y desorganización del soporte y de las tareas asignadas al cargo.
Hacker, cracker	Ingeniería social. Intrusión al sistema. Acceso no autorizado al sistema.
Terrorismo/Vandalismo	Daño de equipos. Penetración en el sistema. Manipulación del sistema. Fraude

Crimen computacional	Fraude. Spoofing. Intrusión al sistema. Soborno de información.
Espionaje Industrial	Ventaja política Explotación económica. Robo de información. Intrusión en información del personal. Ingeniería social. Penetración del sistema. Acceso no autorizado al sistema.
Personal y usuarios internos (deficiente capacitación, descontento, negligentes, deshonestidad, o empleados cesados)	Chantaje. Abuso de computación. Fraude y robo. Pérdida de la confidencialidad e integridad de los datos. Destrucción negligente de equipos, cables y datos. Ingreso de código malicioso (Virus, caballo de Troya, bomba lógica, etc.). Venta/intercambio de información. Fallas en el sistema. Intrusión en el sistema. Sabotaje del sistema. Acceso no autorizado al sistema.
Incorrecta Administración del Sistema y de los derechos de acceso	Fallas en el sistema. Accesos no autorizados. Pérdida de confidencialidad. Uso innecesario de recursos.
Robo	Costos de reposición en equipos. Sistema no operativo. Falta de disponibilidad. Pérdida de confidencialidad.
Amenazas Técnicas	
FUENTE DE AMENAZA	**ACCIONES DE LA AMENAZA**
Falla de un componente	Falla en las operaciones del sistema. Daño en equipos.
Falla del proveedor de servicio de Internet	Suspensión de servicios dependientes del servicio de Internet.
Operación incorrecta de controles existentes	Falta de protección de los activos de información. Daño en los activos de información. Accesos no autorizados. Fallas en el sistema.
Vulnerabilidades o errores en software	Fallas en el sistema. Falta de protección de los activos de información. Pérdida de la confidencialidad, integridad y disponibilidad de la información.
Virus, bombas lógicas, caballo de Troya, código malicioso	Falla en el sistema. Pérdida de la confidencialidad, integridad y disponibilidad de la información.

Amenazas Organizacionales	
FUENTE DE AMENAZA	**ACCIONES DE LA AMENAZA**
Falta o insuficiencia de normas	Deficiencias en la gestión de recursos y operaciones. Pérdida de confidencialidad de la información.
Monitoreo insuficiente de las medidas de seguridad de TI	Incidentes que afecten a la imagen y seguridad de la corporación.
Uso no controlado de activos de información	Falla o daño de los activos de información
Configuraciones débiles a cambios en el uso de TI	Falla en el sistema
Falta de, o inadecuada documentación	Daños en la operación. Gestión inadecuada.
La estrategia para la red y el sistema de gestión no está establecida	Problemas de instalación, configuración y operación de nuevos componentes en la red y en el sistema de gestión. Conexiones a la red no autorizadas. Secuestro de conexiones de red.
Falta de estaciones de trabajo con estándares de configuración	Dificultad en la instalación y mantenimiento. Dificultad en la seguridad de la información.
Falta o insuficiente Gestión de las Seguridad de la Información	Falta de responsabilidad del personal. Inadecuado soporte de gestión. Inadecuados requerimientos estratégicos y conceptuales. Inversión subutilizada o mal encaminada. Falla para actualizar los procesos de TI
Falta de licencias de software propietario y/o violación de derechos de autor	Sanciones legales a la corporación.

Tabla 2.7 Lista de Amenazas

2.3.1.1.3 Identificación de Existencia de Controles

Por el momento la CORPAIRE no posee documentación sobre controles, mucho menos de planes de implementación del tratamiento del riesgo.

2.3.1.1.4 Identificación de Vulnerabilidades

Las vulnerabilidades son explotadas por las amenazas. La identificación de vulnerabilidades está dada en función de la lista de amenazas y la lista de activos.

La presencia de una vulnerabilidad no causa daño en sí, se necesita de una amenaza presente para explotarla. Una vulnerabilidad que no tiene una amenaza correspondiente no podrá exigir la aplicación de un control, pero debe ser reconocida y monitoreada para cambios.

Cabe señalar que un control mal implementado, en mal funcionamiento o usado incorrectamente, podría ser una vulnerabilidad. Un control puede ser eficaz o ineficaz dependiendo del ambiente en el que opera. Por el contrario, una amenaza que no tiene una vulnerabilidad correspondiente no puede ocasionar un riesgo.

A continuación se muestra la tabla 2.8 con las vulnerabilidades y amenazas.

Amenazas Naturales o Ambientales		
No.	**VULNERABILIDAD**	**FUENTE DE DE AMENAZA**
1	No se posee un Plan de Recuperación de Desastres.	Sismo
2	No se posee generadores de energía eléctrica de respaldo.	Tormenta Eléctrica
3	No hay instalaciones de dispositivos apropiados para la eliminación y prevención de incendios.	Falla Eléctrica
4	No se posee generadores de energía eléctrica de respaldo.	
5	No se posee sistemas de calefacción y de aire acondicionado.	Polución
6	No se posee sistemas de calefacción y de aire acondicionado.	Humedad/Corrosión
7	No existen controles suficientes para la seguridad física.	Condiciones de trabajo inadecuadas
8	No se posee sistemas de calefacción y de aire acondicionado.	

Amenazas Humanas o Accidentales		
No.	**VULNERABILIDAD**	**FUENTE DE DE AMENAZA**
1	No existen controles para asegurar la integridad de la información.	Hacker, cracker
2	Se puede ejecutar de forma remota código arbitrario.	
3	No existen controles adecuados de acceso lógico al sistema, los cuales limiten a los usuarios a funciones y transacciones autorizadas.	
4	Existen vulnerabilidades de software que permiten obtener información de la red y redireccionar maliciosamente el tráfico.	
5	Las versiones de sistema operativo y paquetes usados en la ejecución de servicios y aplicaciones no están actualizados y/o libres de errores o fallas.	
6	El personal no ha recibido un adecuado entrenamiento para cumplir con sus responsabilidades respecto a seguridad de la información.	Personal y usuarios internos (deficiente capacitación, descontento, negligentes, deshonestidad, o empleados cesados)
7	No existen controles adecuados de acceso lógico al sistema, los cuales limiten a los usuarios a funciones y transacciones autorizadas.	
8	No existen controles para asegurar la integridad de la información.	
9	Las versiones de sistema operativo y paquetes usados en la ejecución de servicios y aplicaciones no están actualizados y/o libres de errores o fallas.	
10	Se puede obtener información de claves de red, sistema operativo, servicios que se están ejecutando, programas instalados en equipos, e información sensible mediante el acceso a recuros o por escaneos de red.	Incorrecta Administración del Sistema y de los derechos de acceso
11	Muchas instalaciones de programas se las realiza por defecto, sin modificar las configuraciones predeterminadas.	
12	Las configuraciones de algunos servicios se realizan sin tomar en cuenta la seguridad de la información.	
13	Las cuentas de usuario invitado se encuentran habilitadas y no son monitoreadas.	
14	No se toma en cuenta el rol y las obligaciones del personal para aplicar controles.	
15	No existe documentación suficiente que explique el uso de los activos de información.	
16	No se protege suficientemente la integridad de la información y de las aplicaciones.	
17	No se controla permanentemente el acceso a los activos de información.	Robo

Amenazas Técnicas		
No.	**VULNERABILIDAD**	**FUENTE DE DE AMENAZA**
1	No se realiza una correcta prueba de todo el hardware y software nuevo, antes de su aprobación y puesta en producción.	Falla de un componente
2	No están identificadas las operaciones críticas y sus respaldos.	
3	Pérdida del servicio de Internet.	Falla del proveedor de servicio de Internet
4	Falta o carencia de revisión de los controles de seguridad del sistema.	Operación incorrecta de controles existentes
5	Las versiones de sistema operativo y paquetes usados en la ejecución de servicios y aplicaciones no están actualizados y/o libres de errores o fallas.	Vulnerabilidades o errores en software
6	No se administra correctamente el sistema para reducir posibles vulnerabilidades.	
7	No se actualiza y/o revisa el software de detección y eliminación de virus.	Virus, bombas lógicas, caballo de Troya, código malicioso
Amenazas Organizacionales		
No.	**VULNERABILIDAD**	**FUENTE DE DE AMENAZA**
1	Control deficiente en el acceso a la información mendiante los servicios, y recursos compartidos.	Falta o insuficiencia de normas
2	No se ha elaborado un Plan de Contingencias.	
3	No existe un procesos formal de respuesta a incidentes.	
4	No existen especificaciones apropiadas de las obligaciones del personal.	
5	No se actualiza constantemente los sistemas operativos, ni los aplicaciones.	
6	No existe documentación suficiente que explique el uso de los activos de información.	Uso no controlado de activos de información
7	No se controla permanentemente el acceso a los activos de información.	
8	No se evualúa periódicamente los riesgos de seguridad de la información.	Configuraciones débiles a cambios en el uso de TI
9	No se revisan los control de seguridad.	
10	No existen un control de cambios.	
11	El personal no tiene conciencia del riesgo de los sistemas a su cargo.	Falta de, o inadecuada documentación
12	No se tiene una metodología para el ciclo de vida del desarrollo de sistemas.	
13	La administración no garantiza que las acciones correctivas estén implementadas acertadamente.	La estrategia para la red y el sistema de gestión no está establecida
14	No están identificadas las operaciones críticas y sus respaldos.	
15	No existen los controles suficientes para proteger la integridad de la aplicación.	

16	No se tiene suficientes rastros de auditoría.	Falta o insuficiente Políticas de Seguridad de la Información
17	No se realiza evaluaciones del riesgo de seguridad de la información periódicamente, tampoco se ha determinado un nivel de riesgo aceptable.	
18	No existe una propuesta o documento alguno de Políticas de Seguridad de la Información.	
19	No existen controles adecuados de acceso lógico al sistema, los cuales limiten a los usuarios a funciones y transacciones autorizadas.	
20	Falta o carencia de revisión de los controles de seguridad del sistema.	
21	No se tiene una metodología para el ciclo de vida de del desarrollo de sistemas.	
22	Algunos computadores no poseen licencias de software propietario instalado.	Falta de licencias de software propietario y/o violación de derechos de autor

Tabla 2.8 Lista de Vulnerabilidades

2.3.1.2 Análisis de Riesgo

2.3.1.2.1 Metodología para el análisis de riesgo

El análisis de riesgos puede llevarse a cabo en diversos grados de detalle dependiendo de la criticidad de los activos, medida de vulnerabilidades y prioridad de incidentes en la organización. Una metodología de análisis de riesgo puede ser cualitativa o cuantitativa.

En la práctica, a menudo se utiliza primero el análisis cualitativo para obtener una indicación general del nivel de riesgo y revelar los riesgos importantes. En este proyecto de tesis se utilizará el método cualitativo.

Análisis de Riesgo Cualitativo

El análisis de riesgo cualitativo usa una escala de calificación de atributos para describir la magnitud de las consecuencias potenciales (por ejemplo baja, media y alta) y la probabilidad de esas consecuencias. Una ventaja del análisis

cualitativo es su facilidad de comprensión por todo el personal, mientras que una desventaja es la dependencia de la elección subjetiva de la escala.

2.3.1.2.2 Determinación del nivel de riesgo

Para determinar el nivel de riesgo se considerará la probabilidad de un incidente basado en el impacto del negocio. La probabilidad de un incidente está dada por una amenaza que explota a la vulnerabilidad con una cierta probabilidad.

La siguiente tabla 2.9 mapea la probabilidad de un incidente contra el impacto del negocio relacionada con el incidente.

	Impacto		
Probabilidad de Amenaza	**Bajo**	**Medio**	**Alto**
Alta	Bajo	Medio	Alto
Media	Bajo	Medio	Medio
Baja	Bajo	Bajo	Bajo

Tabla 2.9 Valor del Riesgo

La determinación de la probabilidad de ocurrencia para una amenaza, se muestra en la tabla 2.10.

AMENAZAS	
Probabilidad de ocurrencia	**DESCRIPCIÓN**
Baja	Hay una baja probabilidad. La frecuencia de ocurrencia es una vez al año o superior.
Media	Hay una moderada probabilidad, posiblemente. La frecuencia de ocurrencia es una vez cada medio año o menos.
Alta	Hay una alta probabilidad. La frecuencia de ocurrencia es una vez al mes o más.

Tabla 2.10 Probabilidad de ocurrencia de una amenaza

2.3.2 EVALUACIÓN DEL RIESGO

2.3.2.1 Criterios de evaluación del riesgo.

Los criterios de evaluación del riesgo considerarán lo siguiente:

- Las características de la seguridad de la información del activo de información involucrado.
- Sensibilidad de la información.

2.3.2.2 Criterios de Impacto

Los criterios de impacto estarán dados en términos del grado de daño a la corporación, causado por un acontecimiento de seguridad de la información. Para aquello se considerará las violaciones a los principios básicos de la seguridad de la información como son la pérdida de la confidencialidad, integridad y disponibilidad.

La descripción del valor de la confidencialidad se describe en la tabla 2.11.

CONFIDENCIALIDAD	
ESCALA	**DESCRIPCIÓN**
Baja	Puede ser revelado y proporcionado a terceros. Si el contenido fuera revelado, hubiera pequeños efectos en las operaciones de la organización.
Media	Puede ser revelado y proporcionado dentro de la corporación a partes específicas o departamentos, no disponible a terceros. Si el contenido fuera revelado, hubiera pequeños efectos en las operaciones de la organización.
Alta	Puede ser revelado y proporcionado a partes específicas. Si el contenido fuera revelado, hubiera un efecto irrecuperable de las operaciones de la organización.

Tabla 2.11 Valoración de la Confidencialidad

La descripción del valor de la integridad se describe en la tabla 2.12.

INTEGRIDAD	
ESCALA	**DESCRIPCIÓN**
Baja	No necesaria. Usado solo para consulta. No tiene posibles problemas
Media	Necesaria. Si el contenido fuera falsificado, hubiera problemas, pero estos no afectarían mucho a las operaciones de la corporación.
Alta	Importante. Si la integridad se perdiera, hubiera un efecto fatal para las operaciones de la corporación.

Tabla 2.12 Valoración de la Integridad

La descripción del valor de la disponibilidad se describe en la tabla 2.13.

DISPONIBILIDAD	
ESCALA	**DESCRIPCIÓN**
Baja	Si la información no llegara a estar disponible, no hubiera efectos en las operaciones.
Media	Si la información no llegara a estar disponible, hubiera algun efecto en las operaciones. Sin embargo, métodos alternativos pudieran ser usados para las operaciones, o los procesos podrían ser demorados hasta que la información este disponible.
Alta	Si la información no estuviera disponible cuando sea necesitada, hubiera un efecto fatal en las operaciones de la corporación.

Tabla 2.13 Valoración de la Disponibilidad

Para valorar la sensibilidad de la información se tomó en cuenta la experiencia profesional y laboral del personal técnico del Departamento de Tecnología de la corporación así como del autor, que tiene bajo su responsabilidad algunos activos de información. Esta valoración está dada en función de los tres principios básicos de la seguridad de la información, descritas en las tres tablas anteriores.

A continuación en la tabla 2.14 se describe la sensibilidad de la información para cada tipo de activo de información.

Tipo de Activo de Información	Característica de la Seguridad de la Información	Categoría de Sensibilidad
Procesos y actividades del negocio	Confidencialidad	Media
	Integridad	Alta
	Disponibilidad	Alta
Información	Confidencialidad	Alta
	Integridad	Media
	Disponibilidad	Alta
Hardware	Confidencialidad	Alta
	Integridad	Alta
	Disponibilidad	Alta
Software	Confidencialidad	Media
	Integridad	Alta
	Disponibilidad	Alta
Red	Confidencialidad	Alta
	Integridad	Alta
	Disponibilidad	Alta
Recurso Humano	Confidencialidad	Media
	Integridad	Baja
	Disponibilidad	Media

Tabla 2.14 Sensibilidad de la Información por cada Tipo de Activo de Información

En la tabla 2.15 se establecen los riesgos existentes junto con su valoración, en función de la probabilidad y el análisis de impacto que cada riesgo presenta.

Amenazas Naturales o Ambientales					
No.	**Vulnerabilidad**	**Fuente de Amenaza**	**Probabilidad**	**Impacto**	**Valoración del Riesgo**
1	No se posee un Plan de Recuperación de Desastres.	Sismo	Baja	Alto	Bajo
2	No se posee generadores de energía eléctrica de respaldo.	Tormenta Eléctrica	Media	Alto	Medio
3	No hay instalaciones de dispositivos apropiados para la eliminación y prevención de incendios.	Falla Eléctrica	Baja	Bajo	Bajo
4	No se posee generadores de energía eléctrica de respaldo.		Media	Alto	Medio
5	No se posee sistemas de calefacción y de aire acondicionado.	Polución	Media	Bajo	Bajo
6	No se posee sistemas de calefacción y de aire acondicionado.	Humedad/Corrosión	Baja	Bajo	Bajo
7	No existen controles suficientes para la seguridad física.	Condiciones de trabajo inadecuadas	Baja	Bajo	Bajo
8	No se posee sistemas de calefacción y de aire acondicionado.		Baja	Bajo	Bajo
Amenazas Humanas o Accidentales					
No.	**Vulnerabilidad**	**Fuente de Amenaza**	**Probabilidad**	**Impacto**	**Valoración del Riesgo**
1	No existen controles para asegurar la integridad de la información.	Hacker, cracker	Media	Alto	Medio
2	Se puede ejecutar de forma remota código arbitrario.		Baja	Medio	Bajo

3	No existen controles adecuados de acceso lógico al sistema, los cuales limiten a los usuarios a funciones y transacciones autorizadas.		Baja	Bajo	Bajo
4	Existen vulnerabilidades de software que permiten obtener información de la red y redireccionar maliciosamente el tráfico.		Baja	Medio	Bajo
5	Las versiones de sistema operativo y paquetes usados en la ejecución de servicios y aplicaciones no están actualizadas y/o libres de errores o fallas.		Media	Medio	Medio
6	El personal no ha recibido un adecuado entrenamiento para cumplir con sus responsabilidades respecto a seguridad de la información.	Personal y usuarios internos (deficiente capacitación, descontento, negligentes, deshonestidad, o empleados cesados)	Media	Alto	Medio
7	No existen controles adecuados de acceso lógico al sistema, los cuales limiten a los usuarios a funciones y transacciones autorizadas.		Media	Medio	Medio
8	No existen controles para asegurar la integridad de la información.		Media	Medio	Medio

9	Las versiones de sistema operativo y paquetes usados en la ejecución de servicios y aplicaciones no están actualizadas y/o libres de errores o fallas.		Alta	Medio	Medio
10	Se puede obtener información de claves de red, sistema operativo, servicios que se están ejecutando, programas instalados en equipos, e información sensible mediante el acceso a recursos o por escaneos de red.	Incorrecta Administración del Sistema y de los derechos de acceso	Baja	Medio	Bajo
11	Muchas instalaciones de programas se las realiza por defecto, sin modificar las configuraciones predeterminadas.		Alta	Medio	Medio
12	Las configuraciones de algunos servicios se realizan sin tomar en cuenta la seguridad de la información.		Alta	Alto	Alto
13	Las cuentas de usuarios tipo invitado se encuentran habilitadas y no son monitoreadas.		Alta	Medio	Medio
14	No se toma en cuenta el rol y las obligaciones del personal para aplicar controles.		Baja	Bajo	Bajo

15	No existe documentación suficiente que explique el uso de los activos de información.		Media	Bajo	Bajo
16	No se protege suficientemente la integridad de la información y de las aplicaciones.		Baja	Bajo	Bajo
17	No se controla permanentemente el acceso a los activos de información.	Robo	Baja	Medio	Bajo
Amenazas Técnicas					
No.	**Vulnerabilidad**	**Fuente de Amenaza**	**Probabilidad**	**Impacto**	**Valoración del Riesgo**
1	No se realiza una correcta prueba de todo el hardware y software nuevo, antes de su aprobación y puesta en producción.	Falla de un componente	Media	Medio	Medio
2	No están identificados las operaciones críticas y sus respaldos.		Media	Alto	Medio
3	Pérdida del servicio de Internet.	Falla del proveedor de servicio de Internet	Baja	Alto	Bajo
4	Falta o carencia de revisión de los controles de seguridad del sistema.	Operación incorrecta de controles existentes	Media	Medio	Medio
5	Las versiones de sistema operativo y paquetes usados en la ejecución de servicios y aplicaciones no están actualizadas y/o libres de errores o fallas.	Vulnerabilidades o errores en software	Alta	Medio	Medio

6	No se administra correctamente el sistema para reducir posibles vulnerabilidades.		Media	Medio	Medio
7	No se actualiza y/o revisa el software de detección y eliminación de virus.	Virus, bombas lógicas, caballo de Troya, código malicioso	Alta	Medio	Medio
Amenazas Organizacionales					
No.	**Vulnerabilidad**	**Fuente de Amenaza**	**Probabilidad**	**Impacto**	**Valoración del Riesgo**
1	Control deficiente en el acceso a la información mediante los servicios, y recursos compartidos.	Falta o insuficiencia de normas	Alta	Medio	Medio
2	No se ha elaborado un Plan de Contingencias.		Alta	Alto	Alto
3	No existe un proceso formal de respuesta a incidentes.		Media	Medio	Medio
4	No existen especificaciones apropiadas de las obligaciones del personal.		Media	Bajo	Bajo
5	No se actualiza constantemente los sistemas operativos, ni los aplicaciones.		Baja	Bajo	Bajo
6	No existe documentación suficiente que explique el uso de los activos de información.	Uso no controlado de activos de información	Media	Medio	Medio
7	No se controla permanentemente el acceso a los activos de información.		Baja	Bajo	Bajo

8	No se evalúa periódicamente los riesgos de seguridad de la información.	Configuraciones débiles a cambios en el uso de TI	Alta	Medio	Medio
9	No se revisan los controles de seguridad.		Baja	Medio	Bajo
10	No existe un control de cambios.		Baja	Medio	Bajo
11	El personal no tiene conciencia del riesgo de los sistemas a su cargo.	Falta de, o inadecuada documentación	Baja	Bajo	Bajo
12	No se tiene una metodología para el ciclo de vida de del desarrollo de sistemas.		Alta	Medio	Medio
13	La administración no garantiza que las acciones correctivas estén implementadas acertadamente.	La estrategia para la red y el sistema de gestión no está establecida	Alta	Medio	Medio
14	No están identificados las operaciones críticas y sus respaldos.		Alta	Medio	Medio
15	No existen los controles suficientes para proteger la integridad de la aplicación.		Media	Medio	Medio
16	No se tiene suficientes rastros de auditoría.	Falta o insuficiente Políticas de Seguridad de la Información	Baja	Bajo	Bajo
17	No se realiza evaluaciones del riesgo de seguridad de la información periódicamente, tampoco se ha determinado un nivel de riesgo aceptable.		Alta	Medio	Medio

18	No existe una propuesta o documento alguno de Políticas de Seguridad de la Información.		Baja	Medio	Bajo
19	No existen controles adecuados de acceso lógico al sistema, los cuales limiten a los usuarios a funciones y transacciones autorizadas.		Media	Bajo	Bajo
20	Falta o carencia de revisión de los controles de seguridad del sistema.		Media	Bajo	Bajo
21	No se tiene una metodología para el ciclo de vida de del desarrollo de sistemas.		Alta	Medio	Medio
22	Algunos computadores no poseen licencias de software propietario instalado.	Falta de licencias de software propietario y/o violación de derechos de autor	Baja	Bajo	Bajo

Tabla 2.15 Valoración del Riesgo

Una de las opciones para el tratamiento del riesgo es el aplicar controles y uno de estos es el aplicar políticas. Como parte fundamental de esta tesis se elaborará una propuesta de Políticas de Seguridad de la Información para mitigar los riesgos, estas políticas estarán alineadas con la misión y objetivos del Departamento de Tecnología de la CORAIRE.

CAPÍTULO 3

ELABORACIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

3.1 DETERMINACIÓN Y JUSTIFICACIÓN DEL MARCO DE TRABAJO A UTILIZAR

3.1.1 MARCOS DE TRABAJO PARA LA ELABORACIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Así como existe una multiplicidad de marcos de trabajo para el Análisis y Evaluación de Riesgos, hay una gran cantidad y variedad de marcos de trabajo para la Elaboración de la Políticas de Seguridad de la Información. Estos se fundamentan en los principios básicos de la seguridad de la información como son la Integridad, Disponibilidad y Confidencialidad.

En el plan de tesis presentado y aprobado para el desarrollo de este proyecto, dentro de la justificación metodológica se menciona el uso del marco de referencia propuesto por SANS Security Policy Project, que ofrece plantillas, guías, recomendaciones y mejores prácticas para la Elaboración de las Políticas de Seguridad de la Información, sin embargo es necesario citar adicionalmente dos marcos de trabajo para comparar y justificar su uso.

3.1.1.1 EL INSTITUTO SANS

El Instituto SANS (**S**ysAdmin **A**udit, **N**etworking and **S**ecurity Institute) es una institución sin fines de lucro creada en 1989, con sede en Bethesda (Maryland, Estados Unidos) y que agrupa a más de 165.000 profesionales de la seguridad informática (consultores, administradores de sistemas, universitarios, agencias gubernamentales, etc.) en todo el mundo.

Sus principales objetivos son:

- Reunir información sobre todo lo referente a seguridad informática (sistemas operativos, routers, firewalls, aplicaciones, IDS, etc.).

- Ofrecer capacitación y certificación en el ámbito de la seguridad informática.

De igual manera, el Instituto SANS es una universidad formativa en el ámbito de las tecnologías de seguridad. Es una referencia habitual en la prensa sobre temas de auditoría informática.

El Instituto SANS provee plantillas para la elaboración de Políticas de Seguridad de la Información, estas son una recopilación de documentos que forman un conjunto de mejores prácticas y se constituyen en la base esencial para la elaboración de dichas políticas.

Como resumen de este marco de trabajo se presenta un listado de las principales ventajas y desventajas. Tal como se muestra en tabla 3.1.

VENTAJAS
Fácil de adaptar a un plan de políticas especifico de una organización
Rápido desarrollo y aplicación de Políticas de Seguridad
Posee plantillas de políticas, que cumplen requerimientos de marcos de referencia como ISO 27001, ITIL, COBIT, etc.
Posee la mayor colección de documentos de investigación sobre Seguridad de la Información.
Es un estándar internacional, lo que le faculta mayor aceptación.
No tiene costo
Es certificable
DESVENTAJAS
No posee herramientas para su implementación
No está muy difundida en el Ecuador

Tabla 3.1 Ventajas y Desventajas de SANS Security Policy Project

3.1.1.2 ISO/IEC 27002:2005

Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a

seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. La norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005.

Los once dominios son:

a. **Política de Seguridad:** documento de política de seguridad y su gestión.
b. **Organización de la Seguridad de la Información:** organización interna, terceros.
c. **Gestión de Activos:** responsabilidad sobre los activos; clasificación de la información.
d. **Seguridad de los Recursos Humanos:** antes del empleo, durante el empleo, cese de empleo o cambio de puesto de trabajo.
e. **Seguridad Física y del Entorno:** áreas seguras, seguridad de los equipos.
f. **Gestión de Comunicaciones y Operaciones:** responsabilidades y procedimientos de operación, gestión de la provisión de servicios por terceros, planificación y aceptación del sistema, protección contra código malicioso y descargable, copias de seguridad, gestión de la seguridad de redes, manipulación de los soportes, intercambio de información, servicios de comercio electrónico, supervisión.
g. **Control de Acceso:** requisitos de negocio para el control de acceso, gestión de acceso de usuario, responsabilidades de usuario, control de acceso a la red, control de acceso al sistema operativo, control de acceso a las aplicaciones y a la información, ordenadores portátiles y teletrabajo.
h. **Adquisición, desarrollo y mantenimiento de sistemas de información:** requisitos de seguridad de los sistemas de información, tratamiento correcto de las aplicaciones, controles criptográficos, seguridad de los archivos del sistema, seguridad en los procesos de desarrollo y soporte, gestión de la vulnerabilidad técnica.
i. **Gestión de los incidentes de Seguridad de la Información:** notificación de eventos y puntos débiles de la seguridad de la información, gestión de incidentes de seguridad de la información y mejoras.
j. **Gestión de la continuidad del negocio:** aspectos de la seguridad de la información en la gestión de la continuidad del negocio.

k. Cumplimientos: cumplimiento de los requisitos legales, cumplimiento de las políticas y normas de seguridad y cumplimiento técnico, consideraciones sobre las auditorías de los sistemas de información.

Como resumen de esta norma se presenta un listado de las principales ventajas y desventajas. Tal como se muestra en la tabla 3.2.

VENTAJAS
Es un estándar adoptado en nuestro país
Señala la posibilidad de determinar un objetivo específico de la norma, para una mejor comprensión.
Fácil de adaptar a un plan específico de políticas
Aprovecha al máximo la funcionalidad y ventajas de ISO 27001
Es un estándar internacional, lo que le faculta mayor aceptación.
Modificación completa con herramientas de edición estándar HTML.
DESVENTAJAS
Acceder a los documentos de la norma tiene un costo
No tiene como objetivos de seguridad la trazabilidad.
No es certificable

Tabla 3.2 Ventajas y Desventajas de ISO/IEC 27002:2005

3.1.1.3 NIST 800-12: AN INTRODUCTION TO COMPUTER SECURITY: THE NIST HANDBOOK

Este estándar provee asistencia en el aseguramiento de recursos computacionales basados en software, hardware e información, mediante la explicación de conceptos importantes, consideraciones de costos e interrelaciones de los controles de seguridad. Ilustra los beneficios de los controles de seguridad, las principales técnicas o acercamientos para cada control y consideraciones importantes relacionadas.

Este documento provee una amplia apreciación de la seguridad computacional para ayudar a los lectores a entender sus necesidades de componente de seguridad y desarrollar un acercamiento cabal para la selección de los

controles de seguridad apropiados. No describe los pasos detallados necesarios para implementar un programa de seguridad computacional, proveer procedimientos de implementación detallados para los controles de seguridad o dar asistencia para auditar la seguridad de sistemas específicos.

El propósito de este documento no es especificar requerimientos, pero si discutir los beneficios de varios controles de sistemas de seguridad y situaciones en las cuales su aplicación podría ser apropiada.

Este escrito acoge los siguientes temas:

1. Introducción
2. Elementos de la Seguridad Computacional
3. Roles y Responsabilidades
4. Amenazas comunes: Una vista resumida
5. Políticas de Seguridad Computacional
6. Administración del programa de seguridad computacional
7. Administración del riesgo de la seguridad computacional
8. Seguridad y planeamiento en el ciclo de vida de un sistema computacional
9. Garantía
10. Problemas de personal o usuario
11. Preparación para contingencias y desastres
12. Tratamiento de incidentes de seguridad computacional
13. Conocimiento, entrenamiento y educación
14. Consideraciones de seguridad en soporte computacional y operaciones
15. Seguridad física y ambiental
16. Identificación y autenticación
17. Control de acceso lógico
18. Pistas de auditoría
19. Criptografía
20. Evaluando y mitigando los riesgos para un sistema computacional hipotético.

Como resumen de este marco de trabajo se presenta un listado de las principales ventajas y desventajas. Tal como se muestra en la tabla 3.3.

VENTAJAS
Provee procedimientos de implementación detallados para los controles de seguridad o de asistencia para auditar la seguridad de sistemas específicos.
Trata los beneficios de varios controles de sistemas de seguridad y situaciones en las cuales su aplicación podría ser apropiada.
Pertenece a NIST, Instituto de Estándares líder en los Estados Unidos.
DESVENTAJAS
No posee herramientas para su implementación
No describe los pasos detallados necesarios para implementar un programa de seguridad computacional
No especifica requerimientos.
No está muy difundido en el Ecuador

Tabla 3.3 Ventajas y Desventajas de NIST 800-12

3.1.2 SELECCIÓN DEL MARCO DE TRABAJO A UTILIZAR

Luego de citar los marcos de trabajo para la elaboración de las políticas de seguridad de la información, se realiza la selección en base a cinco parámetros que son necesarios y que debe cumplir la metodología a utilizar.

A continuación se describen los cinco parámetros o factores determinantes para la selección del marco de trabajo a utilizar.

1. Cumplimiento de los requerimientos de otros marcos de referencia como ISO 27001, COBIT, ITIL, etc.
2. Es un estándar reconocido en Ecuador
3. Rápido y fácil desarrollo y aplicación de las políticas
4. Es certificable
5. Es gratis su uso

A cada uno de estos factores se asignó un peso (valor ponderado) de 0.20, que sumados alcanzan el valor de 1. Entonces se calificó con un valor de 1 a 10 a cada factor para obtener un valor total por cada marco de trabajo y así poder realizar la comparación.

A continuación se visualiza la tabla 3.4 con el análisis de comparación de los tres marcos de referencia.

ANÁLISIS DE COMPARACIÓN								
FACTORES DETERMINANTES		PESO	SANS		ISO 27002		NIST 800-12	
			CALF	VALOR	CALF	VALOR	CALF	VALOR
1	Cumple requerimientos de otros marcos de referencia	0,2	10	2	10	2	5	1
2	Estándar reconocido en Ecuador	0,2	1	0,2	10	2	1	0,2
3	Rápido desarrollo de las políticas	0,2	10	2	10	2	8	1,6
4	Certificable	0,2	10	2	1	0,2	1	0,2
5	Uso Gratuito	0,2	10	2	1	0,2	10	2
	Total	**1,0**		**8,2**		**6,4**		**5,0**

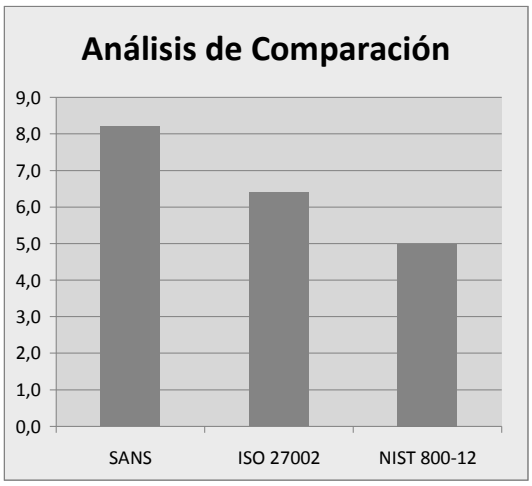

Tabla 3.4 Análisis de Comparación de los marcos de trabajo

Del análisis de comparación de los tres marcos de trabajo, se puede notar que SANS Security Policy Project cumple con todos los parámetros determinantes para realizar la elaboración de las políticas de seguridad de la información.

Antes de describir la metodología a utilizar, citaremos las etapas necesarias para el desarrollo de políticas de seguridad.

3.2 ETAPAS DE DESARROLLO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN [4]

Existen 11 etapas que deben realizarse a través del ciclo de vida de una política y que pueden ser agrupadas en 4 fases que son: Fase de Desarrollo, Fase de Implementación, Fase de Mantenimiento y Fase de Eliminación. Ver la figura 3.1.

El alcance de esta tesis contempla las etapas de Creación y Revisión. Sin embargo, para tener una idea clara de todo el ciclo de vida del desarrollo de una política, se describen cada una de las fases y etapas.

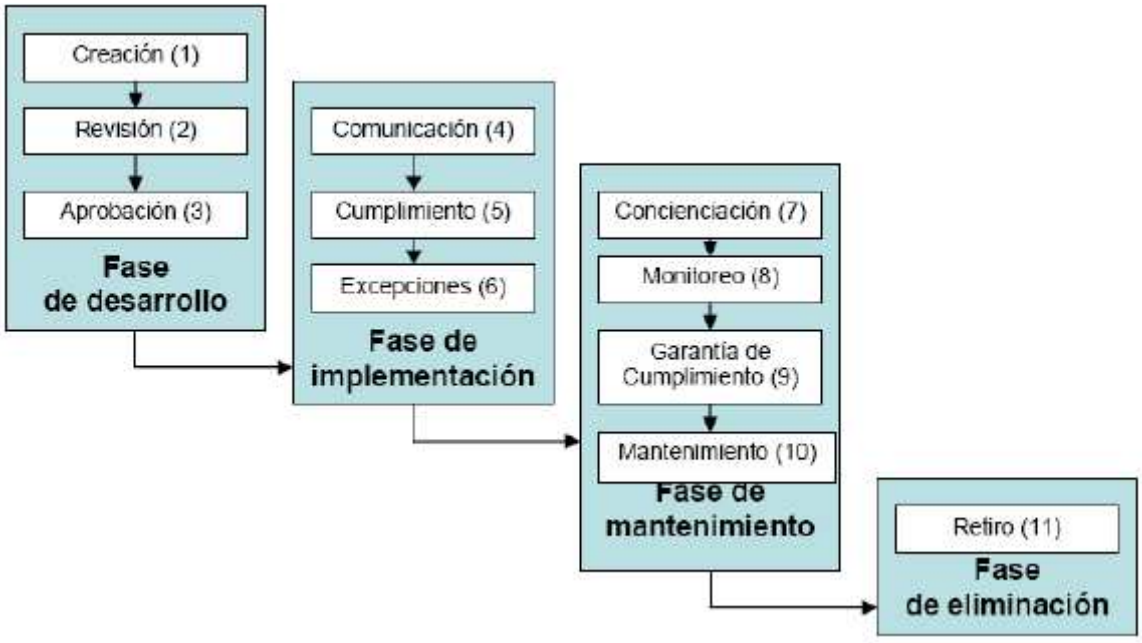

Figura 3.1 Ciclo de Vida de Políticas de Seguridad

Fuente: Guía para elaboración de Políticas de Seguridad. Patrick D. Howard

[4] Tomado de: Guía para elaboración de Políticas de Seguridad. Patrick D. Howard

3.2.1 FASE DE DESARROLLO

Creación (1)

Este primer paso implica identificar la necesidad de crear la política; determinar el alcance de la aplicabilidad de la política, los roles y las responsabilidades de la aplicación de la política y garantizar la factibilidad de su implementación.

Revisión (2)

Remitir al Director Ejecutivo de la CORPAIRE para su evaluación antes de su aprobación final. Se presenta la política a los revisores, de manera formal o informal.

Aprobación (3)

El objetivo es obtener el apoyo del Director Ejecutivo de la CORPAIRE, para la aprobación y oficialización de la política.

3.2.2 FASE DE IMPLEMENTACION

Comunicación (4)

La política debe ser difundida a todo el personal de la corporación o a quienes se vean afectados directamente por la política (proveedores, contratistas, usuarios de cierto servicio, etc.).

Cumplimiento (5)

Ejecución de la política. Trabajar con jefes o directores departamentales de la corporación, para dilucidar cuál es la mejor manera de implementar la política; asegurando que la política sea entendida, implementarla, monitorearla, hacer seguimiento, reportar su cumplimiento y medir el impacto de la política en las operaciones de la corporación.

Excepciones (6)

No todas las políticas pueden ser acatadas de la manera como inicialmente se

planificó. Cuando los casos lo ameriten, es probable que se requieran de excepciones a la política para permitir el no cumplimiento de la política.

3.2.3 FASE DE MANTENIMIENTO

Concienciación (7)

Esfuerzos continuos para garantizar que las personas estén conscientes de la política así como también facilitar su cumplimiento. Determinar los métodos de concienciación más efectivos, tales como reuniones informativas, cursos de entrenamiento, correos electrónicos, etcétera. También el desarrollo y difusión de material de concienciación tales como presentaciones, circulares, etc.

Monitoreo (8)

Seguir y reportar la efectividad de los esfuerzos en el cumplimiento de la política.

Garantía de Cumplimiento (9)

Determinar la acción correctiva a una violación de la política, con el objetivo de prevenir que vuelva a ocurrir. Las acciones pueden ser revisión y mejoramiento de los procesos, actualización de tecnología, y acciones disciplinarias.

Mantenimiento (10)

Garantizar la vigencia y la integridad de la política. Hacer seguimiento a las tendencias de cambios (en tecnología, en procesos, en las personas, en la organización, en el enfoque de la corporación, etc.) y que pueden afectar la política. Esta etapa también garantiza la disponibilidad e integridad de la política a través de un control de versiones.

3.2.4 FASE DE ELIMINACIÓN

Retiro (11)

Cuando una política ha cumplido con su objetivo y ya no es necesaria debe ser

retirada. Esta función se realiza para evitar confusión. Se debe archivar y documentar la información del motivo del retiro.

3.3 DECLARACION DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN A ELABORAR

El Instituto SANS tiene como objetivo principal el de proveer las recomendaciones y las mejores prácticas para el desarrollo de las Políticas de Seguridad de la Información, para este proceso recomienda el uso de plantillas de políticas que han sido elaboradas y probadas por experimentados profesionales en seguridad de la información.

3.3.1 POLÍTICAS EN BASE AL ANÁLISIS DE RIESGOS

A continuación se visualiza la tabla 3.5 Políticas de Seguridad según el Análisis de Riesgos, en la cual se listan las políticas de seguridad que deben ser declaradas.

Amenazas Naturales o Ambientales				
No.	**Vulnerabilidad**	**Fuente de Amenaza**	**Valoración del Riesgo**	**Política de Seguridad**
1	No se posee un Plan de Recuperación de Desastres.	Sismo	Bajo	● Política de Evaluación de Riesgos.
2	No se posee generadores de energía eléctrica de respaldo.	Tormenta Eléctrica	Medio	● Política de Evaluación de Riesgos.
3	No hay instalaciones de dispositivos apropiados para la eliminación y prevención de incendios.	Falla Eléctrica	Bajo	● Política de Evaluación de Riesgos.
4	No se posee generadores de energía eléctrica de respaldo.		Medio	● Política de Evaluación de Riesgos.
5	No se posee sistemas de calefacción y de aire acondicionado.	Polución	Bajo	● Política de Evaluación de Riesgos.
6	No se posee sistemas de calefacción y de aire acondicionado.	Humedad /Corrosión	Bajo	● Política de Evaluación de Riesgos.
7	No existen controles suficientes para la seguridad física.	Condiciones de trabajo inadecuadas	Bajo	● Política de Uso Adecuado.
8	No se posee sistemas de calefacción y de aire acondicionado.		Bajo	● Política de Evaluación de Riesgos

Amenazas Humanas o Accidentales				
No.	**Vulnerabilidad**	**Fuente de Amenaza**	**Valoración del Riesgo**	**Política de Seguridad**
1	No existen controles para asegurar la integridad de la información.	Hacker, cracker	Medio	● Política de Uso Adecuado. ● Política de Sensibilidad de la Información. ● Política de Acceso a Internet. ● Política de Correo Electrónico. ● Política de reenvío de correo electrónico. ● Política de retención de correo electrónico. ● Política de seguridad de la zona desmilitarizada DMZ ● Política de uso de líneas telefónicas para transmisión de datos. ● Política de conexión y acceso telefónico dial-in. ● Política de uso de Dispositivos de Comunicación Personal y voicemail. ● Política de red privada virtual (VPN). ● Política de comunicación Inalámbrica. ● Política de Red de Área Local Virtual VLAN.
2	Se puede ejecutar de forma remota código arbitrario.		Bajo	Política de Acceso Remoto. Política de seguridad de enrutadores.
3	No existen controles adecuados de acceso lógico al sistema, los cuales limiten a los usuarios a funciones y transacciones autorizadas.		Bajo	Política de Contraseñas. Política de seguridad de servidores.
4	Existen vulnerabilidades de software que permiten obtener información de la red y redireccionar maliciosamente el tráfico.		Bajo	● Política de instalación de software. ● Política de seguridad de enrutadores.
5	Las versiones de sistema operativo y paquetes usados en la ejecución de servicios y aplicaciones no están actualizadas y/o libres de errores o fallas.		Medio	● Política de instalación de software.

6	El personal no ha recibido un adecuado entrenamiento para cumplir con sus responsabilidades respecto a seguridad de la información.	Personal y usuarios internos (deficiente capacitación, descontento, negligentes, deshonestidad, o empleados cesados)	Medio	● Política de Uso Adecuado
7	No existen controles adecuados de acceso lógico al sistema, los cuales limiten a los usuarios a funciones y transacciones autorizadas.		Medio	● Política de Contraseñas. ● Política de seguridad de servidores.
8	No existen controles para asegurar la integridad de la información.		Medio	● Política de Sensibilidad de la Información.
9	Las versiones de sistema operativo y paquetes usados en la ejecución de servicios y aplicaciones no están actualizadas y/o libres de errores o fallas.		Medio	● Política de instalación de software.
10	Se puede obtener información de claves de red, sistema operativo, servicios que se están ejecutando, programas instalados en equipos, e información sensible mediante el acceso a recursos o por escaneos de red.	Incorrecta Administración del Sistema y de los derechos de acceso	Bajo	● Política de Contraseñas. ● Política de instalación de software. ● Política de Sensibilidad de la Información.
11	Muchas instalaciones de programas se las realiza por defecto, sin modificar las configuraciones predeterminadas.		Medio	● Política de instalación de software.
12	Las configuraciones de algunos servicios se realizan sin tomar en cuenta la seguridad de la información.		Alto	● Política de Sensibilidad de la Información.
13	Las cuentas de usuarios tipo invitado se encuentran habilitadas y no son monitoreadas.		Medio	● Política de Contraseñas.
14	No se toma en cuenta el rol y las obligaciones del personal para aplicar controles.		Bajo	● Política de Uso Adecuado.
15	No existe documentación suficiente que explique el uso de los activos de información.		Bajo	● Política de Uso Adecuado. ● Política de Ética.
16	No se protege suficientemente la integridad de la información y de las aplicaciones.		Bajo	● Política de Sensibilidad de la Información.
17	No se controla permanentemente el acceso a los activos de información.	Robo	Bajo	● Política de Uso Adecuado.

Amenazas Técnicas				
No.	**Vulnerabilidad**	**Fuente de Amenaza**	**Valoración del Riesgo**	**Política de Seguridad**
1	No se realiza una correcta prueba de todo el hardware y software nuevo, antes de su aprobación y puesta en producción.	Falla de un componente	Medio	● Política de bases de datos de credenciales. ● Política de instalación de software.
2	No están identificados las operaciones críticas y sus respaldos.		Medio	● Política de seguridad de servidores.
3	Pérdida del servicio de Internet.	Falla del proveedor de servicio de Internet	Bajo	● Política de seguridad de servidores. ● Política de seguridad de enrutadores.
4	Falta o carencia de revisión de los controles de seguridad del sistema.	Operación incorrecta de controles existentes	Medio	● Política de Uso Adecuado.
5	Las versiones de sistema operativo y paquetes usados en la ejecución de servicios y aplicaciones no están actualizadas y/o libres de errores o fallas.	Vulnerabilidades o errores en software	Medio	● Política de instalación de software. ● Política de bases de datos de credenciales.
6	No se administra correctamente el sistema para reducir posibles vulnerabilidades.		Medio	● Política de Uso Adecuado
7	No se actualiza y/o revisa el software de detección y eliminación de virus.	Virus, bombas lógicas, caballo de Troya, código malicioso	Medio	● Política de uso de antivirus. ● Política de protección de servidores contra el Malware. ● Política de uso de dispositivos de almacenamiento removible.
Amenazas Organizacionales				
No.	**Vulnerabilidad**	**Fuente de Amenaza**	**Valoración del Riesgo**	**Política de Seguridad**
1	Control deficiente en el acceso a la información mediante los servicios, y recursos compartidos.	Falta o insuficiencia de normas	Medio	● Política de Uso Adecuado. ● Política de Acceso Remoto. ● Política de la Extranet.
2	No se ha elaborado un Plan de Contingencias.		Alto	● Política de evaluación de riesgos.
3	No existe un proceso formal de respuesta a incidentes.		Medio	● Política de evaluación de riesgos.
4	No existen especificaciones apropiadas de las obligaciones del personal.		Bajo	● Política de Uso Adecuado. ● Política de Ética.
5	No se actualiza constantemente los sistemas operativos, ni los aplicaciones.		Bajo	● Política de bases de datos de credenciales.
6	No existe documentación suficiente que explique el uso de los activos de información.	Uso no controlado de activos de información	Medio	● Política de Uso Adecuado.
7	No se controla permanentemente el acceso a los activos de información.		Bajo	● Política de Uso Adecuado.

8	No se evalúa periódicamente los riesgos de seguridad de la información.	Configuraciones débiles a cambios en el uso de TI	Medio	● Política de evaluación de riesgos.
9	No se revisan los controles de seguridad.		Bajo	● Política de Uso Adecuado.
10	No existe un control de cambios.		Bajo	● Política de Sensibilidad de la Información. ● Política de instalación de software.
11	El personal no tiene conciencia del riesgo de los sistemas a su cargo.	Falta de, o inadecuada documentación	Bajo	● Política de Uso Adecuado. ● Política de Ética.
12	No se tiene una metodología para el ciclo de vida de del desarrollo de sistemas.		Medio	● Política de Uso Adecuado. ● Política de Ética.
13	La administración no garantiza que las acciones correctivas estén implementadas acertadamente.	La estrategia para la red y el sistema de gestión no está establecida	Medio	● Política de Uso Adecuado. ● Política de Seguridad de redes LAN.
14	No están identificados las operaciones críticas y sus respaldos.		Medio	● Política de seguridad de servidores.
15	No existen los controles suficientes para proteger la integridad de la aplicación.		Medio	● Política de Sensibilidad de la Información.
16	No se tiene suficientes rastros de auditoría.	Falta o insuficiente Políticas de Seguridad de la Información	Bajo	● Política de escaneo y auditoría de vulnerabilidades.
17	No se realiza evaluaciones del riesgo de seguridad de la información periódicamente, tampoco se ha determinado un nivel de riesgo aceptable.		Medio	● Política de escaneo y auditoría de vulnerabilidades. ● Política de evaluación de riesgos.
18	No existe una propuesta o documento alguno de Políticas de Seguridad de la Información.		Bajo	● Política de Uso Adecuado.
19	No existen controles adecuados de acceso lógico al sistema, los cuales limiten a los usuarios a funciones y transacciones autorizadas.		Bajo	● Política de Cifrado Aceptable. ● Política de Contraseñas.
20	Falta o carencia de revisión de los controles de seguridad del sistema.		Bajo	● Política de evaluación de riesgos.
21	No se tiene una metodología para el ciclo de vida de del desarrollo de sistemas.		Medio	● Política de Uso Adecuado.
22	Algunos computadores no poseen licencias de software propietario instalado.	Falta de licencias de software propietario y/o violación de derechos de autor	Bajo	● Política de instalación de software.

Tabla 3.5 Políticas de Seguridad según el Análisis de Riesgos

A continuación un listado que resume las Políticas de Seguridad a ser declaradas.

Listado de Políticas a ser descritas

Política de Uso Adecuado
Política de Correo Electrónico
Política de reenvío de correo electrónico
Política de retención de correo electrónico
Política de auditoría con escaneo de la vulnerabilidad
Política de evaluación de riesgos
Política de Sensibilidad de la Información
Política de credenciales de bases de datos
Política de instalación de software
Política de Acceso a Internet
Política de protección de servidores contra el Malware
Política de uso de antivirus
Política de seguridad de la zona desmilitarizada DMZ
Política de uso de líneas telefónicas para transmisión de datos
Política de conexión y acceso telefónico dial-in
Política de uso de Dispositivos de Comunicación Personal y Buzones de Voz
Política de uso de dispositivos de almacenamiento removible
Política de Cifrado Aceptable
Política de Contraseñas
Política de seguridad de servidores
Política de seguridad de enrutadores
Política de Red Privada Virtual (VPN)
Política de Acceso Remoto
Política de la Extranet
Política de comunicación Inalámbrica
Política de Seguridad de redes LAN internas
Política de Red de Área Local Virtual (VLAN)
Política de Ética

3.4 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA CORPAIRE

3.4.1 POLÍTICA DE USO ADECUADO

1.0 PROPÓSITO

El objetivo de esta política es establecer los parámetros de uso adecuado de los activos de información en la CORPAIRE. Estas reglas se han establecido para proteger tanto al usuario del activo de información como a la CORPAIRE. El uso indebido de los activos de información expone a la CORPAIRE a riesgos como ataques de virus, vulnerabilidad de los sistemas, redes y servicios, robo de información, además de problemas legales.

2.0 ALCANCE

Su alcance se aplica a empleados, contratistas, consultores, pasantes, y otros usuarios que utilicen los activos de información de la CORPAIRE. Esta política se aplica a todos los activos de información que es de propiedad de la CORPAIRE.

3.0 POLÍTICA

3.1 Uso general y Propiedad

1. Mientras el Departamento de Tecnología responsable de administrar la red de la CORPAIRE provea un nivel razonable de privacidad, los usuarios deben ser conscientes que los datos que crean ellos en los sistemas de la corporación son propiedad de la CORPAIRE. Debido a la necesidad de proteger la red de la CORPAIRE, el Departamento de Tecnología no puede garantizar la confidencialidad de la información almacenada en cualquier dispositivo de red que pertenezca a la corporación.

2. Los empleados son responsables de buen juicio respecto al uso personal de manera razonable. Es responsabilidad de los departamentos crear normas y procedimientos necesarios para el uso adecuado de los activos de información. Si no existen tales normas, los empleados deben consultar a su jefe inmediato.

3. El Departamento de Tecnología responsable de administrar las seguridades de la red de la CORPAIRE, tiene la autorización de controlar los equipos, sistemas y tráfico de la red en cualquier momento.

4. El Departamento de Tecnología de la CORPAIRE se reserva el derecho de realizar auditorías de las redes y sistemas de manera periódica, para garantizar el cumplimiento de esta política.

3.2 Seguridad y Propiedad de la Información

1. La información contenida en las redes y los sistemas relacionados debe ser clasificada como confidencial o no confidencial. Algunos ejemplos de la información confidencial pueden ser: las estrategias corporativas, secretos comerciales, base de datos de vehículos, listas de clientes y datos de investigación. Los empleados deben tomar todas las medidas necesarias para evitar el acceso no autorizado a esta información.

2. Conservar las contraseñas seguras y no compartir cuentas. Los usuarios autorizados son responsables de la seguridad de sus cuentas y contraseñas. Las contraseñas de sistemas y servidores deberán cambiarse trimestralmente y las contraseñas de usuarios cada seis meses.

3. Todas las estaciones de trabajo deben ser aseguradas con un protector de pantalla, protegido con contraseña y con la función de activación automática por inactividad de 10 minutos o menos. Así también debe salir de la sesión, mediante la combinación de las teclas (**control-alt-suprimir**), cuando el usuario ya no lo vaya a usar. El protector de pantalla debe ser el que autoriza la corporación.

4. Todas las estaciones de trabajo deben estas configuradas con un fondo de escritorio autorizado por la corporación.

5. Se debe tener cuidado especial con los computadores portátiles, debido a que la información contenida en estos es muy vulnerable.

6. Los mensajes creados por parte de los empleados desde las cuentas de correo de la CORPAIRE, para los grupos de noticias, deberán contener una cláusula que indique que las opiniones expresadas en estos están bajo su responsabilidad, y no necesariamente refleja una posición oficial de la CORPAIRE, a menos que la publicación lo amerite.

7. Todos los mensajes creados por parte de los empleados desde las cuentas de correo de la CORPAIRE, deberán contener una nota de aviso de confidencialidad. Por ejemplo: “Este mensaje (Incluido sus documentos adjuntos) contiene información confidencial dirigida a una persona o propósito específico y se encuentra protegido por la ley. Si usted no es el destinatario original, por favor debe eliminarlo. Cualquier copia, distribución o cualquier acción basada en el mismo se encuentra estrictamente prohibida por la ley”.

El objetivo de este tipo de advertencias es crear un ambiente de privacidad de las comunicaciones y el secreto profesional a terceros, alertando a quien recibe el correo que, en caso de no ser el destinatario, ya sea por error, equivocación u otra razón, debe borrarlo.

8. Todos los computadores utilizados por el empleado y que estén conectados a la red de la CORPAIRE, ya sean de propiedad del empleado o de la CORPAIRE, deberán ser escaneados con el programa de antivirus aprobado y con su base de datos de virus actualizada.

9. Los empleados deben tener mucho cuidado al abrir archivos adjuntos de correo electrónico recibidos de remitentes desconocidos, estos pueden contener virus, bombas de correo, código troyano, etc.

3.3 Uso Inaceptable

Se prohíben las siguientes actividades, sin embargo los empleados pueden quedar exentos de estas restricciones solo en el caso del ejercicio de su legítima responsabilidad laboral.

A continuación las actividades que entran en la categoría de uso inaceptable.

Actividades del Sistema y la Red

Sin excepción alguna están estrictamente prohibidas las siguientes actividades:

1. Copia no autorizada de material protegido por derechos de autor, esto incluye la digitalización y distribución de fotografías de revistas, libros, música u otras fuentes con derechos de autor. También está prohibida la instalación de cualquier software protegido por derechos de autor para los cuales la CORPAIRE no tenga una licencia original.

2. Introducción de programas maliciosos en la red o servidor (por ejemplo virus, gusanos, caballos de Troya, spam, etc.).

3. Ceder el uso de contraseñas o cuentas personales a otros. Esto incluye a la familia y otros miembros de la familia cuando se está trabajando en la casa.

4. Utilizar los activos de información de la CORPAIRE para la transmisión de material que viole las leyes de la jurisdicción local y material de acoso sexual.

5. Efectuar violaciones de seguridad o interrupciones a la red de comunicación. Las “violaciones de seguridad” incluyen, pero no se limitan a, tener acceso a datos a los cuales el empleado no está expresamente autorizado, a menos que estas actividades estén incluidas dentro del ámbito de sus funciones ordinarias. Para fines de esta sección, "interrupción" incluye, pero no se limita, al sniffing de la red, inundaciones ping, spoofing de paquetes, denegación de servicio, y el forjado de enrutamiento de información para propósitos maliciosos.

6. Escaneo de puertos está expresamente prohibido, a menos que esta actividad se notifique previamente al Administrador de Seguridad.

7. Ejecutar cualquier forma de monitoreo de la red, la cual intercepte datos que nos sean de propiedad del empleado, a menos que esta actividad sea parte del trabajo normal del mismo.

8. Evadir la autenticación de usuario o la seguridad de cualquier computador, red o cuenta.

9. El uso de cualquier programa, script, comando, o enviar mensajes de cualquier tipo con la intención de interferir o desactivar una sesión del usuario, a través de cualquier medio local o por medio de la red.

Actividades de Correo electrónico y comunicación

1. Envío de mensajes de correo electrónico no solicitado, incluyendo el envío de "correo basura" o de material publicitario a personas que no hayan solicitado dicho material (spam).

2. Cualquier tipo de acoso a través del correo electrónico, mensajería personal, teléfono, o búsqueda de personas.

3. El uso no autorizado o falsificación de la información del encabezado del correo electrónico.

4. Solicitud de correo electrónico para otra dirección de correo electrónico, con la intención de acosar o para recibir respuestas.

5. El crear o reenviar "cartas en cadena", "Ponzi" o esquemas de “pirámide” de cualquier tipo.

6. El uso de correo electrónico no solicitado generado dentro de la red de la CORPAIRE en nombre de los proveedores de servicios, o para publicitar cualquier servicio auspiciado por la CORPAIRE.

Blogging

1. El Blogging de los empleados, usando los activos de información de la CORPAIRE, también está sujeto a las condiciones y restricciones establecidas en esta Política. El uso ocasional y limitado de los sistemas de la CORPAIRE para participar en blogging es aceptable, siempre que se haga de manera

profesional y responsable, no viole las políticas de la CORPAIRE, no perjudique los intereses de la corporación, y no interfiera con las actividades normales del empleado. El Blogging desde los sistemas de la CORPAIRE estará sujeto a monitoreo.

2. Las políticas de información confidencial de la CORPAIRE también aplican para el blogging. Tanto así, que los empleados están prohibidos a revelar cualquier información confidencial de la CORPAIRE, información propietaria de secretos de marca o cualquier otro material cubierto por las Políticas de Información Confidencial de la CORPAIRE cuando se use el blogging.

3. Los empleados no realizarán ningún blogging que puedan dañar o empañar la imagen, reputación y/o las buenas relaciones de la CORPAIRE o de cualquiera de sus empleados. Los empleados también están prohibidos de hacer cualquier comentario de discriminación, menosprecio, difamación o acoso cuando usen el blogging.

4. Los empleados no pueden atribuir a su declaraciones personales como opiniones de la CORPAIRE, cuando usen el blogging. Si un empleado está expresando sus creencias y/o dictámenes en blogs, el empleado no puede representarse a sí mismo como un empleado o representante de la CORPAIRE. Los empleados deben asumir todos los riesgos asociados con blogging.

5. Además de seguir todas las leyes relacionadas con el manejo y divulgación de los derechos de autor o exportación de materiales controlados; las marcas, logotipos y cualquier propiedad intelectual de la CORPAIRE no pueden ser utilizadas en ninguna actividad relacionada al blogging.

4.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.2 POLÍTICA DE CORREO ELECTRÓNICO

1.0 PROPÓSITO

Prevenir y evitar una afectación de la imagen pública de la CORPAIRE cuando se envía correo electrónico hacia fuera de la misma, porque el público en general tiende a pensar que el mensaje expresa una declaración oficial de la CORPAIRE.

2.0 ALCANCE

Esta política cubre el uso apropiado de cualquier correo electrónico que es remitido desde una dirección de correo electrónico de la CORPAIRE y se aplica a todos los empleados, contratistas, consultores, pasantes, y otros usuario de la CORPAIRE.

3.0 POLÍTICA

3.1 Uso no autorizado

El correo electrónico no debe ser usado para crear o distribuir cualquier tipo de mensaje discriminativo u ofensivo. Los empleados que reciban correo electrónico con este tipo de contenido, deben informar inmediatamente a su jefe inmediato o al Departamento de Tecnología.

3.2 Uso personal

Utilizar de manera razonable el correo electrónico para uso personal es aceptable. Advertencias sobre virus u otros programas maliciosos y envíos masivos de correos desde la CORPAIRE deberán ser aprobados por el Departamento de Tecnología antes de su envío. Estas restricciones también aplica al reenvío del correo recibido por un empleado de la CORPAIRE.

3.3 Monitoreo

Los empleados de la CORPAIRE no tendrán privacidad sobre la información que ellos almacenen, envíen o reciban en el sistema de correo electrónico de la corporación. El Departamento de Tecnología puede monitorear el correo electrónico sin previo aviso.

4.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.3 POLÍTICA DE REENVÍO AUTOMÁTICO DE CORREO ELECTRÓNICO

1.0 PROPÓSITO

Prevenir la divulgación no autorizada o inadvertida de información confidencial de la CORPAIRE.

2.0 ALCANCE

Esta política cubre el reenvío automático de correo electrónico, previniendo la transmisión inadvertida de información confidencial por parte de todos los empleados, contratistas, consultores, pasantes, y otros usuarios de la CORPAIRE.

3.0 POLÍTICA

Todos los empleados, contratistas, consultores, pasantes, y otros usuarios de la CORPAIRE, deben tener mucho cuidado al enviar un correo electrónico desde la red interna de la corporación a una red externa. A menos que sea aprobado por el Departamento de Tecnología, un correo de la CORPAIRE no deberá ser enviado automáticamente a un destinatario externo.

Correo electrónico con información sensible no deberá ser enviado por ningún medio, a menos que este sea crítico para el negocio y esté cifrado en concordancia con la Política de Cifrado Aceptable.

4.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.4 POLÍTICA DE RETENCIÓN DE CORREO ELECTRÓNICO

1.0 PROPÓSITO

Esta política permite ayudar a los empleados a determinar qué tipo de información enviada o recibida debe ser retenida y por cuánto tiempo.

2.0 ALCANCE

Esta política aplica a todo correo electrónico que contenga información sensible de la CORPAIRE. La información del correo de la corporación esta categorizada dentro de cuatro clasificaciones principales con directrices de retención:

- Correo administrativo (4 años)
- Correo fiscal (4 años)
- Correo en general (1 año)
- Correo temporal (Se debe retener hasta leerlo y luego borrarlo)

3.0 POLÍTICA

3.1 Correo Administrativo

Se considera correo administrativo a todo aquel relacionado con políticas internas, días festivos, horarios de ingreso y salida, código de uso de uniformes del personal, normas de comportamiento en el lugar de trabajo y cualquier cuestión de tipo legal. Para asegurar que este tipo de correo sea retenido, se deberá crear una cuenta para estos fines, por ejemplo admin@corpaire.org. Cuando se envíe un correo electrónico y se desee que sea retenido, se deberá enviar una copia (cc) a la cuenta de correo antes descrita. Esta retención será administrada por el Departamento de Tecnología.

3.2 Correo Fiscal

El correo fiscal de la CORPAIRE es todo aquel relacionado con ingresos y gastos de la corporación. Para asegurar que este tipo de correo sea retenido, se deberá crear una cuenta para estos fines, por ejemplo el buzón fiscal@corpaire.org. Cuando se envíe un correo electrónico y se desee que sea retenido, se deberá enviar una copia (cc) a la cuenta de correo antes descrita. Esta retención será administrada por el Departamento de Tecnología.

3.3 Correo en general

El correo en general de la CORPAIRE cubre toda la información que se relaciona con la interacción del cliente y las decisiones operativas de la corporación. El empleado es responsable de la retención del correo electrónico de este tipo.

3.4 Correo temporal

El correo temporal es la categoría más común e incluye el correo electrónico personal, requerimientos de recomendación u opinión, actualizaciones e informes de estado.

3.5 Recuperación del correo electrónico desde los medios de respaldo

Una de las responsabilidades del Departamento de Tecnología es respaldar el servidor de correo. No se modificará o eliminará información del correo electrónico de los medios de respaldo.

4.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.5 POLÍTICA DE AUDITORÍA CON ESCANEO DE LA VULNERABILIDAD

1.0 PROPÓSITO

El propósito de esta política es establecer un acuerdo respecto del escaneo de la seguridad de la red, que ofrece la auditoría interna o externa de la CORPAIRE. Estas auditorías deberán utilizar software aprobado para realizar escaneos electrónicos en los computadores de red, firewalls o en cualquier sistema de la CORPAIRE.

Los objetivos de las auditorías son:

- Asegurar los tres principios básicos de seguridad de la información como son la integridad, confidencialidad y disponibilidad.

- Investigar que ante posibles incidentes de seguridad se garantice el cumplimiento de las políticas de seguridad de la CORPAIRE.
- Monitorear que las actividades de los usuarios o sistemas sean las apropiadas.

2.0 ALCANCE

La presente política aplica a todos los computadores y equipos de comunicación que se encuentren en las instalaciones de la CORPAIRE, incluidos los que no pertenezcan a esta.

3.0 POLÍTICA

Con el propósito de realizar una auditoría, se permitirá que los auditores puedan acceder a las redes y firewalls de la CORPAIRE. La corporación suministrará los protocolos, direcciones y conexiones de red necesarios para que los auditores utilicen el Software para el escaneo de la red.

Este acceso puede incluir:

- Nivel de acceso de usuario y/o sistema para cualquier computadora o equipo de comunicación.
- Acceso a la información (electrónica, almacenada en discos duros, documentos impresos en papel, etc.) que pueda ser creada, transmitida o almacenada en los equipos de la CORPAIRE.
- Acceso a las instalaciones de trabajo.
- Acceso para monitorear y registrar el tráfico de la red de la CORPAIRE.

3.1 Degradación y/o Interrupción del Servicio.

El escaneo puede afectar el desempeño y/o disponibilidad de la red. La CORPAIRE libera de cualquier responsabilidad a los auditores por daños que puedan surgir por las restricciones de disponibilidad de la red a causa de la exploración de la red, a menos que tales daños sean el resultado de la negligencia o conducta intencional de los auditores.

3.2 Punto de contacto con el usuario durante el proceso de escaneo.

La CORPAIRE deberá identificar por escrito a una persona, la cual tendrá contacto con el equipo de auditores si tienen alguna pregunta o requieran ayuda sobre resultados durante la evaluación.

3.3 Período de escaneo.

La CORPAIRE y los auditores elaborarán un documento que establezca las fechas en las cuales el equipo de auditoría pueda ejecutar el propósito de esta política.

4.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.6 POLÍTICA DE EVALUACIÓN DE RIESGOS

1.0 PROPÓSITO

Empoderar al Departamento de Tecnología de la CORPAIRE para realizar evaluaciones periódicas de riesgos de seguridad de la información, con el objetivo de determinar las áreas de vulnerabilidad e iniciar una remediación apropiada.

2.0 ALCANCE

Las evaluaciones de riesgo pueden ser realizadas por el Departamento de Tecnología de la CORPAIRE o por cualquier otra entidad externa que tenga firmado un Acuerdo de Terceros con la CORPAIRE. Las evaluaciones de riesgos pueden llevarse a cabo en cualquier sistema de información, incluye aplicaciones, servidores y redes, y cualquier proceso o procedimiento inherente al sistema.

3.0 POLÍTICA

La ejecución, desarrollo e implementación de programas de remediación son responsabilidad del Departamento de Tecnología de la CORPAIRE. Es

necesaria la cooperación de los empleados en todo proceso de evaluación de riesgos que se lleve a cabo en los sistemas que están bajo su responsabilidad. Además los empleados deberán trabajar con el equipo responsable del proceso de evaluación de riesgos para desarrollar un plan de remediación.

4.0 PROCESO DE EVALUACIÓN DEL RIESGO

Referirse al Subcapítulo 2.3 VALORACIÓN Y EVALUACIÓN DEL RIESGO.

5.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.7 POLÍTICA DE SENSIBILIDAD DE LA INFORMACIÓN

1.0 PROPÓSITO

La Política de Sensibilidad de la Información tiene como propósito ayudar a los empleados de la CORPAIRE a determinar qué información puede ser divulgada a personas que no son parte de la CORPAIRE, así como la información sensible que no debe ser revelada fuera de la CORPAIRE sin la debida autorización.

Todos los empleados deben familiarizarse con el etiquetado de la información y el manejo de esta política. Las definiciones de niveles de sensibilidad se han creado como orientación sobre las medidas de sentido común que el funcionario puede tomar para proteger la información confidencial de la CORPAIRE. (por ejemplo: No se debe dejar Información confidencial de la CORPAIRE en las salas de conferencia).

2.0 ALCANCE

La información cubierta por esta política incluye, pero no se limita a, información que se guarda o es compartida a través de cualquier medio. Esto

incluye: la información electrónica, la información en papel, así como la información oral o visual (por ejemplo: conferencias telefónicas y de video).

Toda la información de la CORPAIRE está clasificada en dos categorías principales:

- Pública
- Confidencial

Información Pública de la CORPAIRE es aquella que ha sido declarada de dominio público por alguien con la autoridad para hacerlo, y que puede ser distribuida libremente a cualquier persona sin afectar los intereses y propiedad intelectual de la corporación.

La información Confidencial es toda la otra información que no cae en la categoría de pública. Se incluye información que debe ser protegida muy de cerca, como los secretos comerciales, programas de desarrollo, adquisiciones, y otra información esencial para el éxito de la corporación.

La CORPAIRE al ser una corporación municipal debe acatar la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP), es así como cierta información considerada como sensible es categorizada pública. Como por ejemplo los directorios telefónicos, la información corporativa en general, la información del personal, etc.

Existe información confidencial perteneciente a terceros que han confiado en la CORPAIRE y con quienes se ha firmado acuerdos de no divulgación.

3.0 POLÍTICA

Las siguientes políticas de sensibilidad que a continuación se describen, detallan el cómo proteger la información en los varios niveles de sensibilidad. Estas normas son solo una referencia, puede ser necesario tomar medidas más rigurosas o menos estrictas dependiendo de las circunstancias y la naturaleza de la información confidencial de la CORPAIRE.

3.1 Sensibilidad mínima. Información general de la corporación, información de empleados y alguna información técnica.

Políticas de marcado de información en papel o formato electrónico:

Nota: Se pueden utilizar cualquiera de estas marcas con la nota adicional de “Confidencial Terceras Partes”.

El marcado está a discreción del propietario o custodio de la información.

Se puede usar las palabras "Confidencial - CORPAIRE" para marcar, estas deben estar ubicadas en un lugar visible o sobre la información en cuestión.

Otras etiquetas que pueden ser usadas son "Propiedad de la CORPAIRE" u otras marcas similares a discreción de la unidad de negocio o departamento. Sin embargo; si no está presente ninguna marca, se presume que la información es confidencial a menos que se determine por algún empleado de la CORPAIRE con la autoridad para hacerlo, que dicha información es pública

Consideraciones sobre la información de sensibilidad mínima:

Acceso: Tendrán acceso los empleados de la CORPAIRE, contratistas y personas con una necesidad comercial.

Distribución dentro de la CORPAIRE: Es aceptado el correo interno normal, correo electrónico y transmisión electrónica de archivos.

Distribución fuera de la CORPAIRE: Son aceptados operadores de correo normal públicos o privados, métodos aprobados de correo electrónico y transmisión electrónica de archivos.

Distribución electrónica: No existe restricción alguna siempre que los destinatarios hayan sido aceptados previamente.

Almacenamiento: Mantenga fuera de vista de personas no autorizadas, borrar los pizarrones y no dejar información sobre la mesa. Para protegerse de la pérdida de información electrónica, se debe tener controles de acceso individuales siempre y cuando se posible y apropiado.

Eliminación/Destrucción: La información en papel con fecha antigua debe ser depositada en basureros de las instalaciones de la CORPAIRE especialmente marcados; los datos electrónicos antiguos deben ser depurados.

Sanción por divulgación deliberada o involuntaria: Juicio civil o penal en caso de divulgar información confidencial que perjudique los intereses de la corporación, incluyendo el despido.

3.2 Información de Sensibilidad Media. Información comercial, financiera, técnica e información personal.

Políticas de marcado de información en papel o formato electrónico:

Nota: Se puede utilizar cualquiera de estas marcas con la nota adicional "Confidencial Terceras Partes". A medida que el nivel de sensibilidad de la información aumente, es posible que en lugar de marcar la información como "Confidencial – CORPAIRE" o "Propiedad de CORPAIRE", sea necesario etiquetar la información como "Solo para uso interno - CORPAIRE".

Consideraciones sobre la información de sensibilidad media:

Acceso: Tendrán acceso los empleados de la CORPAIRE y personas externas con firmas de acuerdo de no divulgación y que tengan una necesidad comercial.

Distribución dentro de la CORPAIRE: Es aceptado el correo interno normal, correo electrónico y transmisión electrónica de archivos.

Distribución fuera de la CORPAIRE: Son aceptados operadores calificados de correo públicos o privados, correo electrónico y transmisión electrónica de archivos.

Distribución electrónica: No existe restricción alguna siempre que los destinatarios hayan sido aceptados previamente, pero la distribución debe ser encriptada o a través de una conexión privada para aquellos destinatarios ubicados fuera de las instalaciones de la CORPAIRE.

Almacenamiento: Los controles de acceso individual son muy recomendables para la información electrónica.

Eliminación/Destrucción: Depositar en basureros de las instalaciones de la CORPAIRE especialmente marcados; los datos electrónicos deben ser borrados.

Sanción por divulgación deliberada o involuntaria: Juicio civil o penal en caso de divulgar información confidencial que perjudique los intereses de la corporación, incluyendo el despido.

3.3 Información muy sensible

Secretos transaccionales, operacionales, personales, códigos fuentes e información técnica necesaria para las operaciones de la corporación.

Nota: En cualquiera de las marcas la información puede etiquetarse como: "Confidencial - CORPAIRE", "Propiedad registrada y restringida de la CORPAIRE", "Sólo para uso interno de la CORPAIRE". Si este tipo de información lleva estas etiquetas los usuarios deben ser conscientes de que esta información es muy sensible y se debe proteger como tal.

Consideraciones:

Acceso: Tendrán acceso solo aquellos empleados de la CORPAIRE, que tengan firmado y aprobado acuerdos de confidencialidad.

Distribución dentro de la CORPAIRE: Entrega directa, se requiere la firma, sobres con sellos de confidencialidad o métodos electrónicos aprobados de transmisión de archivos.

Distribución fuera de la CORPAIRE: Entrega directa, se requiere la firma, operadores de correo privados aprobados.

Distribución electrónica: No existe restricción para los destinatarios aprobados por la CORPAIRE, pero es muy recomendable que toda la información sea cifrada.

Almacenamiento: Los controles de acceso individual son muy recomendables para la información electrónica. Se suele utilizar la seguridad física, además la información debe ser almacenada en un computador físicamente protegido.

Disposición/Destrucción: Depositar en basureros de las instalaciones de la CORPAIRE especialmente marcados; los datos electrónicos deben ser borrados. Asegúrese de haber borrado o destruido la información.

Sanción por divulgación deliberada: Penalización civil o penal en caso de divulgar información confidencial que perjudique los intereses de la corporación, incluyendo el despido.

4.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.8 POLÍTICA DE CREDENCIALES DE BASES DE DATOS

1.0 PROPÓSITO

Establecer los requisitos para almacenar y recuperar con seguridad los nombres de usuarios y contraseñas de base de datos (credenciales de bases de datos) usados por programas que accederán a una base de datos que corre en la red de la CORPAIRE.

Los programas que se ejecutan en la red de la CORPAIRE, usualmente requieren acceder a uno de los servidores internos de bases de datos. Para acceder a una de estas bases de datos, el programa debe autenticarse en la base de datos mediante la presentación de credenciales aceptables. Los privilegios de base de datos que las credenciales están destinadas a restringir pueden verse comprometidos cuando las credenciales son almacenadas inadecuadamente.

2.0 ALCANCE

Esta política es aplicable a todos aquellos programas de la CORPAIRE que accedan a bases de datos de producción.

3.0 POLÍTICAS

3.1 General

Para que las bases de datos internas de la CORPAIRE sean seguras, el acceso a programas se debe llevar a cabo a través de la autenticación por medio de credenciales. Estas credenciales no deben estar descritas en el cuerpo principal del programa, tampoco deberán ser almacenadas en sitios que se puedan acceder a través de un servidor Web.

3.2 Requerimientos específicos

3.2.1. Almacenamiento de nombres de usuario y contraseñas en la Base de Datos.

- Los nombres de usuario y contraseñas de la base de datos deben ser guardados en un archivo independiente del código del programa. Este archivo no debe permitir ser leído por todos.

- Las credenciales de la base de datos pueden residir en el servidor de base de datos.
- Las credenciales de la base de datos pueden ser almacenadas como parte de un servidor de autenticación, por ejemplo en un servidor LDAP. La autenticación de la base de datos puede ser durante la ejecución de un programa como parte del proceso de autenticación de usuarios ante el servidor de autenticación.
- El paso de autenticación no debe permitir el acceso a la base de datos basándose solamente en la autenticación de un usuario remoto en el host remoto.
- Las contraseñas o frases de paso usadas para el acceso a la base de datos deben cumplir con la *Política de Contraseña*.

3.2.2. Recuperación de nombres de usuario y contraseñas

- Si están almacenados en un archivo que no es parte de código fuente, los nombres de usuario y contraseñas deben ser leídos desde el archivo antes de su uso. Inmediatamente después de la autenticación en la base de datos, la memoria que contiene los nombres de usuario y contraseñas debe ser liberada y limpiada.
- Para los lenguajes que se ejecutan desde el código fuente, el archivo fuente de credenciales no debe residir en el mismo árbol de directorio de archivos ejecutables.

3.3.3. Acceso a la Base de Datos de nombres de usuario y contraseñas

- Cada programa o colección de programas que implementen una determinada función comercial, deben tener una única base de datos de credenciales. No se permite compartir credenciales entre programas.
- Las contraseñas de base de datos usadas por los programas y que permiten niveles de acceso al sistema deben ser definidas por la Política de Contraseñas.
- El grupo de desarrollo debe tener un proceso interno para asegurar que las contraseñas de la base de datos sean controladas y cambiadas de acuerdo con la *Política de Contraseña*. Este proceso debe incluir un

método para restringir la obtención de contraseñas de la base de datos ante personas no autorizadas.

4.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.9 POLÍTICA DE INSTALACIÓN DE SOFTWARE

1.0 PROPÓSITO

Reducir el riesgo de pérdida de funcionalidad de los programas, minimizar la exposición de la información sensible contenida dentro de la red de la CORPAIRE, evitar el riesgo de la introducción de malware y de la ejecución ilegal de software no autorizado.

2.0 ALCANCE

Esta política aplica a todos los computadores, servidores, y otros equipos que funcionan dentro de la red de la CORPAIRE.

3.0 POLÍTICA

Los empleados no pueden instalar software en los equipos de la red de la CORPAIRE. Los requerimientos de nuevo software deberán ser solicitados y aprobados por el jefe inmediato para luego ser enviados al Departamento de Tecnología por escrito o vía correo electrónico para su revisión y opinión sobre su aprobación o no.

El Departamento de Tecnología realizará pruebas del nuevo software para validar compatibilidad con los sistemas operativos, obtendrá las licencias y realizará la instalación, en el caso de aprobación del requerimiento

4.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.10 POLÍTICA DE ACCESO A INTERNET

1.0 PROPÓSITO

Reducir al mínimo: el riesgo de pérdida de funcionalidad de la red de la CORPAIRE, la exposición de la información sensible contenida dentro de la red de la CORPAIRE, el riesgo de introducir virus, la descarga e instalación ilegal de software no autorizado, navegación en páginas clasificadas como prohibidas, el acceso no autorizado y la pérdida de reputación de la Corporación.

2.0 ALCANCE

Esta política se aplica a todos los usuarios de Internet (personas que trabajan para la empresa, incluyendo empleados a tiempo completo y empleados a tiempo parcial, trabajadores contratados, trabajadores temporales de agencias, socios comerciales) que acceden a Internet mediante los recursos de red de la CORPAIRE.

El Acceso a Internet será proporcionado a los usuarios para apoyar actividades comerciales y sólo sobre la base necesaria para realizar su trabajo y funciones profesionales.

Los usuarios de Internet de la corporación deben conocer y cumplir con esta política, y también están obligados a utilizar su sentido común y ejercer su buen juicio mientras utilizan los servicios de Internet.

3.0 SERVICIOS PARA EL USUARIO

Servicios de Internet Permitidos

El Acceso a Internet se proporciona a los usuarios para apoyar las actividades de negocios en el desempeño de sus trabajos y roles profesionales. Los usuarios tendrán la facilidad de usar los siguientes servicios de Internet, de acuerdo a sus necesidades:

- **Correo electrónico**. Enviar y recibir mensajes de correo electrónico hacia o desde el Internet (con o sin documentos adjuntos).

- **Navegación web**. Este servicio es necesario para propósitos de negocio, usando las herramientas de navegación como los protocolos HTTP o HTTPS. Acceso total a Internet, acceso limitado solo a servidores web de empresas públicas.

- **Protocolo de Transferencia de Archivos (FTP).** Enviar y recibir archivos necesarios para fines comerciales de la corporación.

La Dirección del Departamento de Tecnología de la CORPAIRE se reserva el derecho a agregar o eliminar servicios de acuerdo a los cambios o necesidades de la Corporación. Todos los otros servicios serán considerados no autorizados y el acceso hacia o desde el Internet no será permitido.

Solicitud y procedimiento de aprobación.

El Acceso a Internet se proporcionará a los usuarios para apoyar las actividades comerciales de la CORPAIRE y sólo en caso necesario para realizar sus actividades diarias de trabajo.

Como parte del proceso de solicitud de acceso a Internet, el empleado está obligado a leer tanto la Política de Uso de Internet así como otras políticas de seguridad afines a esta. El usuario debe entonces firmar las declaraciones de que entiende y acepta a cumplir con las políticas.

Negación del Servicio.

El Acceso a Internet será negado luego de la terminación del contrato del funcionario o como medida disciplinaria derivadas de la violación de esta política. En el caso de un cambio en la función del cargo y/o transferencia, el acceso original al servicio será suspendido, y sólo publicado nuevamente si es necesario y una nueva solicitud de acceso sea aprobada.

4.0 POLÍTICA

4.1. Uso de Recursos

El Acceso a Internet será aprobado y proporcionado siempre y cuando las necesidades empresariales están identificadas razonablemente. El Servicio de Internet será concedido sobre la base de responsabilidades de trabajo de un empleado. Si un funcionario se cambia a otra unidad de negocios o cambia sus funciones, una nueva petición de acceso a Internet debe presentarse dentro de 5 días.

Los requerimientos de usuarios para el acceso a Internet serán revisados periódicamente por los departamentos de la corporación, para asegurarse de que se continúa con la necesidad de este servicio.

4.2 Uso permitido.

La utilización de Internet es concedida con el único propósito de apoyar a las actividades de la corporación necesarias para llevar a cabo las funciones de trabajo. Todos los usuarios deben seguir los principios corporativos sobre uso de recursos y ejercer buen juicio en el uso de Internet. Las preguntas pueden ser dirigidas al Departamento de Tecnología.

El uso Aceptable de Internet para realizar funciones de trabajo puede incluir:

- Comunicación entre empleados y no empleados para fines comerciales.
- El apoyo técnico para descargar actualizaciones y parches de software.
- Revisión de sitios web de proveedores para información de productos.
- Referencia reglamentaria o información técnica.
- Investigación.

4.3 Uso personal.

Usar recursos informáticos de la corporación y acceder a Internet para fines personales, sin la aprobación del administrador de usuarios, o del director del departamento de TI, puede ser considerado motivo de acción disciplinaria e incluir la terminación laboral.

Todos los usuarios de Internet deben ser conscientes de que la red de la corporación crea un registro de auditoría reflejando solicitud de servicio y es revisado periódicamente.

Los usuarios que seleccionen el Internet para almacenar o transmitir información personal como claves privadas, números de tarjetas de crédito o certificados, lo hacen bajo su propia responsabilidad y riesgo. La empresa no es responsable de cualquier pérdida de información.

5.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.11 POLÍTICA DE PROTECCIÓN DE SERVIDORES CONTRA EL MALWARE

1.0 PROPÓSITO:

Proporcionar una protección adecuada a los servidores de la CORPAIRE contra las amenazas malware tales como virus, gusanos, SPAM y spyware entre otros.

2.0 ALCANCE:

Esta política se aplica a todos los servidores de la red de la CORPAIRE. Se incluye sistemas sobre los cuales la CORPAIRE tiene una obligación contractual de administrar. También se incluye las configuraciones de todos los servidores de uso interno de la CORPAIRE, independientemente de si la CORPAIRE tiene o no una obligación administrativa.

3.0 POLÍTICA:

El administrador de seguridades de la información de la CORPAIRE debe considerar esta política con el fin de determinar cuáles son los servidores que deben tener instalados y configurarlos adecuadamente aplicaciones anti-virus y/o anti-spyware.

3.1 ANTI-VIRUS

Todos los servidores deben tener instalado un antivirus, el cual debe proporcionar protección en tiempo real mediante escaneo de archivos y aplicaciones que se ejecutan en el sistema destino, si se cumple una o más de las siguientes condiciones:

- Los usuarios no administrativos tienen capacidad de acceso remoto
- El sistema es un servidor de archivos.
- Si el acceso de NBT/Microsoft Share está abierto al sistema destino.
- Si el acceso HTTP / FTP está abierto al Internet.
- Si otros protocolos/aplicaciones de riesgo están disponibles a los sistemas destinos desde el Internet a discreción del Administrador de Seguridades de la CORPAIRE.

3.2 ANTI-VIRUS DEL SERVIDOR DE CORREO

Todos los servidores de correo deben tener instalado una aplicación antivirus que analice todo el correo saliente y entrante.

3.3 ANTI-SPYWARE

Todos los servidores deben tener instalada una aplicación anti-spyware que permita protección en tiempo real de cualquier ataque al sistema destino, si se cumple una o más de las siguientes condiciones:

- Cualquier sistema en el cual los usuarios tienen acceso remoto y es permitido cualquier acceso de salida al Internet.
- Cualquier sistema en el que los usuarios tienen la capacidad de instalar software.

3.4 ANTISPAM

Todos los servidores de correo deben tener instalada una aplicación antispam, que permita protección en tiempo real de ataques al sistema. Si se envían mensajes no deseados (SPAM) desde una cuenta del dominio de la CORPAIRE, en la instancia de detección la cuenta será bloqueada

temporalmente y se enviará un correo de advertencia a la cuenta del administrador de seguridad de la información.

4.0 CUMPLIMIENTO

La responsabilidad de llevar a cabo esta política es de todo el personal técnico del Departamento de Tecnología de la CORPAIRE. La responsabilidad de asegurar que los servidores nuevos o existentes permanezcan en cumplimiento de esta política reside en el administrador de seguridades de la información de la CORPAIRE. Cualquier empleado que se encuentre violando esta política puede ser sujeto a medidas disciplinarias, incluyendo la terminación del contrato laboral.

3.4.12 POLÍTICA DE USO DE ANTIVIRUS

1.0 PROPÓSITO

Establecer los requerimientos y procedimientos que deben cumplir todas las computadoras conectadas a la red de la CORPAIRE, para garantizar una eficaz prevención, detección y eliminación de virus.

2.0 ALCANCE

Esta política aplica a todas las estaciones de trabajo conectadas a la red de la CORPAIRE.

3.0 POLÍTICA

Todos las computadoras de la CORPAIRE deben cumplir estas normas, deben estar protegidas por un software anti-virus, el cual debe programarse para ser ejecutado en intervalos de tiempo que no afecten las actividades diarias del usuario. Además se debe actualizar constantemente la base de datos y archivos de patrones de virus. Los computadores infectados con virus deben ser desconectados de la red hasta se encuentren libres de virus.

Se prohíbe cualquier actividad que tenga la intención de crear o distribuir programas maliciosos en la red de la CORPAIRE (por ejemplo: virus, SPAM,

gusanos, troyanos, bombas de correo electrónico, etc.) de acuerdo con la Política de Uso Adecuado.

Procesos recomendados para prevenir problemas de Virus:

- Siempre se debe ejecutar como norma corporativa, el software antivirus que debe estar disponible en el sitio descargas corporativo. Descargar y ejecutar la versión más actual. Descargar e instalar las actualizaciones del software antivirus a medida que ellas estén disponibles.
- Nunca abrir archivos o macros adjuntos a un correo electrónico desde una fuente desconocida, sospechosa o no confiable. Se debe borrar inmediatamente estos tipos de correo con archivos adjuntos, luego borrarlos nuevamente vaciando la carpeta de elementos eliminados o carpeta de reciclaje.
- No reenviar el SPAM, cadenas y todo tipo de correo basura, los mismos que deben ser borrados.
- Nunca descargar archivos desde fuentes sospechosas o desconocidas.
- Evitar el compartir un disco duro dando acceso de lectura/escritura a menos que sea un requerimiento del negocio.
- Siempre se debe escanear los dispositivos removibles (memorias flash, disquetes, etc.) en busca de virus antes de usarlos.
- Respaldar la información crítica y las configuraciones del sistema calendarizadamente y guardar estos respaldos en un lugar seguro.
- Casi todos los días son descubiertos nuevos virus. Chequear periódicamente las actualizaciones para el antivirus.

4.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.13 POLÍTICA DE SEGURIDAD DE LA ZONA DESMILITARIZADA DMZ

1.0 PROPÓSITO

El propósito de esta política es determinar los requerimientos de seguridad de la información que deben cumplir todos los equipos conectados a la red de la CORPAIRE y que están ubicados en la Zona Desmilitarizada (DMZ). Esta política está diseñada para minimizar el riesgo potencial de la pérdida de datos confidenciales o sensibles, propiedad intelectual, daño de la imagen pública, etc., los cuales son causados por el uso no autorizado de los recursos de la CORPAIRE.

Los dispositivos que se enfrentan a Internet y que están ubicados fuera del firewall de la CORPAIRE son considerados parte de la “Zona Desmilitarizada” (DMZ) y están sujetos a esta política. Estos dispositivos son particularmente vulnerables a ataques desde el Internet debido a que están fuera del firewall de la red corporativa.

La política define los siguientes estándares:

- Responsabilidad de propiedad
- Requerimientos de configuración segura
- Requerimientos operacionales
- Requerimientos de control de cambios

2.0 ALCANCE

Todos los equipos y dispositivos localizados en una DMZ y operados por la CORPAIRE, tales como ruteadores, conmutadores, hosts, etc., y registrados en cualquier dominio (DNS) de la CORPAIRE deben seguir esta política. Todo aquel equipamiento nuevo que este bajo el alcance de esta política deberá ser configurado de acuerdo a los documentos de configuración referenciados.

3.0 POLÍTICA

3.1 Propiedad y Responsabilidades

Los equipos y aplicaciones que están dentro del alcance de esta política deben ser administrados por el Departamento de Tecnología de la CORPAIRE.

El Departamento de Tecnología será responsable de lo siguiente:

- Los equipos deben ser registrados en un sistema de gestión de activos de información de la corporación. Para lo cual se requiere la siguiente información:
    - Los responsables de los Host y su ubicación.
    - Hardware y versión del sistema operativo.
    - Funciones Principales y aplicaciones.
    - Grupos de contraseñas para las contraseñas privilegiadas.
- Las interfaces de red deben ser registradas apropiadamente en el Servidor de Nombres de Dominio.
- Los grupos de contraseñas deben ser administrados de acuerdo al proceso de administración de contraseñas.
- Los cambios en equipos existentes o la instalación de nuevos equipos deben seguir las reglas de la corporación o el proceso de gestión de cambios.

Para verificar el cumplimiento de esta política, el Departamento de Tecnología auditará periódicamente los equipos de la DMZ de acuerdo a la *Política de Auditoría*.

3.2 Política de Configuración General

Todos los equipos deben obedecer la siguiente política de configuración:

- El hardware, sistemas operativos, servicios y aplicaciones deben ser aprobados por el Departamento de Tecnología de la CORPAIRE como parte de la fase de pre-producción.
- La configuración de sistema operativo debe hacerse según los estándares de configuración segura.
- Se deben instalar todos los Service Pack o parches recomendados por el vendedor del equipo y el Departamento de Tecnología de la CORPAIRE.

Esto aplica a todos los servicios instalados, aunque estos pueden estar temporal o permanentemente desactivados.

- Los servicios y aplicaciones que no sirvan a los requerimientos corporativos se deben desactivar.
- Se configurarán relaciones de confianza entre sistemas solo en caso de un requerimiento corporativo plenamente justificado y aprobado por el Departamento de Tecnología de la CORPAIRE.
- La administración remota debe realizarse sobre canales seguros (por ejemplo, conexiones de red que usen SSH o IPSEC).
- Toda actualización de contenido de un host debe realizarse sobre canales seguros.
- Deben anotarse los eventos seguridad y rastros de auditoría en archivos tipo logs y auditados por el Departamento de Tecnología de la CORPAIRE. Los eventos de seguridad incluyen (pero no se limitan) a lo siguiente:
    - Fallas de ingreso de Usuarios.
    - Fallas al obtener privilegio de acceso.
    - Violaciones a la Política de Acceso.
- El Departamento de Tecnología de la CORPAIRE aprobará excepciones a la política en caso de ser requerido.

3.3 Procedimientos de Nuevas Instalaciones y Gestión de Cambios

Las nuevas instalaciones y cambios en la configuración de equipos y aplicaciones existentes deben seguir las siguientes políticas/procedimientos:

- Las nuevas instalaciones deben seguir el *Proceso de Instalación de Equipos DMZ*.
- Los cambios de configuración de equipos deben seguir los Procedimientos de Gestión de Cambios (CM) de la corporación.
- El Departamento de Tecnología de la CORPAIRE ejecutará auditorías del sistema y aplicaciones antes de la provisión de nuevos servicios.
- El Departamento de Tecnología de la CORPAIRE deberá aprobar de manera directa o por medio del proceso de CM la configuración de todos los nuevos equipos en producción así como los cambios de configuración.

3.4 Equipos de Proveedores de Servicio Externo

La responsabilidad de proteger los equipos instalados por los proveedores de servicios externos debe estar especificada en el contrato que la CORPAIRE acuerde con el proveedor de servicios.

4.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.14 POLÍTICA DE USO DE LÍNEAS TELEFÓNICAS PARA TRANSMISIÓN DE DATOS

1.0 PROPÓSITO

El propósito de esta política es explicar el uso adecuado de las líneas telefónicas utilizadas en la transmisión de datos y conectadas únicamente a computadores y faxes al interior de la CORPAIRE.

2.0 ALCANCE

Esta política cubre sólo a las líneas telefónicas utilizadas en la transmisión de datos y que se conectan a un equipo al interior de la CORPAIRE. No abarca las líneas de teléfono que están conectadas en los hogares de los empleados, centrales telefónicas, y aquellas líneas usadas para llamadas de emergencia y con propósito de información no corporativa.

3.0 POLÍTICA

3.1 Escenarios e Impacto Comercial

Existen dos escenarios importantes que involucran el uso indebido de las líneas telefónicas, los cuales hay que proteger a través de esta política.

El primero es un atacante externo quien llama a un conjunto de números de línea telefónica con la intención de conectarse a un equipo de la CORPAIRE que tenga instalado un módem. Si el modem responde existe la posibilidad de violar la red interna de la CORPAIRE a través de ese computador no monitoreado. La información de ese computador puede verse comprometida.

Esto conlleva a una pérdida económica al valorar la información corporativa comprometida.

El segundo escenario es la amenaza de que cualquier persona con acceso físico en la CORPAIRE haga uso de un computador de escritorio o de un portátil equipado con un módem. En este caso, el intruso podría tener la capacidad de conectarse a la LAN de la CORPAIRE a través de la conexión Ethernet de dicho computador y hacer una llamada externa a través del modem a algún lugar no monitoreado, con capacidad de enviar información sensible de la CORPAIRE a un lugar desconocido.

A continuación los procedimientos específicos para hacer frente a los riesgos de seguridad referentes a cada uno de esos escenarios.

3.2 Máquinas de fax

Por regla general se aplica lo siguiente:

- Las líneas de fax son de uso exclusivo de la CORPAIRE.
- No existirán líneas de fax instaladas para uso personal.
- El fax debe ser colocado en un lugar físico estratégico.
- A cualquier computador que sea capaz de hacer una conexión de fax no se le proveerá de una línea telefónica para este propósito.

El uso de una línea telefónica para fax está sujeto a que el solicitante cumpla plenamente con los requisitos que se indican a continuación:

- La línea de fax será utilizada solamente para lo que se especifica en la solicitud.
- Sólo las personas autorizadas podrán tener acceso a la línea de fax.
- Cuando la línea no esté en uso debe ser físicamente desconectada del computador.
- Cuando la línea esté en uso, el computador debe estar físicamente desconectado de la red interna de la CORPAIRE.
- La línea se utilizará exclusivamente para actividades de la CORPAIRE y no para actividades personales.

3.3 Conexión de computador a línea telefónica

La política general es que las solicitudes de computadores que deseen conectarse con líneas telefónicas dentro de la CORPAIRE, no sean aprobadas por razones de seguridad. Las líneas telefónicas constituyen una importante amenaza para la seguridad de la información de la CORPAIRE.

3.4 Solicitar una Línea telefónica

Una vez aprobado el requerimiento, la persona que solicite una línea telefónica debe proporcionar la siguiente información al proveedor:

- Una clara y detallada explicación la cual justifique las razones por las que otras conexiones seguras disponibles en la CORPAIRE no se pueden utilizar.
- El objetivo comercial para el cual la línea telefónica se va a utilizar.
- El software y hardware a ser conectado y usado a través de a línea.
- Las conexiones externas a las que el solicitante intente conectarse.

4.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.15 POLÍTICA DE CONEXIÓN Y ACCESO TELEFÓNICO DIAL-IN

1.0 PROPÓSITO

El propósito de esta política es proteger la información electrónica de la CORPAIRE al momento de crear un acceso telefónico dial-in a la red. Aunque este tipo de conexión ya no se utiliza en la corporación ni en la mayoría de las instituciones, es necesario declararla para su conocimiento y difusión.

2.0 ALCANCE

El alcance de esta política es definir apropiadamente el acceso dial-in y el uso por personal autorizado.

3.0 POLÍTICA

Los empleados de la CORPAIRE y terceras partes autorizadas pueden usar conexión dial-in para tener acceso a la red corporativa. Este tipo de conexión debe ser controlada, usando una contraseña de autentificación, la cual deberá ser proporcionada por el Departamento de Tecnología.

Es responsabilidad de los empleados, con privilegios de acceso dial-in, asegurar que la conexión hacia la red de la CORPAIRE no sea utilizada por personas o empleados que no pertenezcan a la corporación para obtener acceso a la información de la CORPAIRE.

El empleado a quien se la ha otorgado privilegios de conexión dial-in debe estar consciente de que esta conexión entre su ubicación y la CORPAIRE es una extensión de la red corporativa y que esto proporciona una entrada potencial a la información sensible de la CORPAIRE.

Nota: Las cuentas dial-in se asignarán en base a las necesidades. La actividad de esta cuenta es monitoreada y si no es usada en un período de seis meses, la cuenta expirará y dejará de funcionar. Si la cuenta dial-in es requerida nuevamente, se debe hacer una solicitud como una nueva cuenta.

4.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.16 POLÍTICA DE USO DE DISPOSITIVOS DE COMUNICACIÓN PERSONALES Y BUZONES DE VOZ

1.0 PROPÓSITO

El propósito de esta política es describir los requerimientos de Seguridad de la Información para los Dispositivo de Comunicación Personales PCDs (**P**ersonal **C**ommunications **D**evices) y para los buzones de voz de la CORPAIRE.

2.0 ALCANCE

Esta política se aplica al uso de cualquier Dispositivo de Comunicación Personal y para buzones de voz otorgados por la CORPAIRE o usados para fines de la Corporación.

3.0 POLÍTICA

3.1 Política de emisión

Los Dispositivos de Comunicación Personal sólo se asignarán a personal de la CORPAIRE que tenga actividades que les obligue a estar en contacto inmediato y frecuente cuando se encuentren fuera de su lugar de trabajo normal. Por ejemplo el personal que trabaja en los operativos en vía pública. Para mejor comprensión de esta política, se definen PCDs a dispositivos inalámbricos portátiles, teléfonos celulares, tarjetas inalámbricas de portátiles y dispositivos busca personsa.

Los Dispositivos de Comunicación Personal pueden ser entregados, para eficiencia operacional, a personal de la CORPAIRE que necesita despachar o realizar actividades críticas relacionadas con la institución de manera inmediata. Estas personas generalmente se encuentran en niveles directivos y de gestión. Además del contacto verbal, es necesario que tengan la capacidad de revisar y tener respuestas documentadas sobre problemas críticos.

3.2 Bluetooth

Dispositivos de manos libres, como Bluetooth, pueden ser asignados a personal autorizado de la CORPAIRE quienes han recibido aprobación. Se debe tener cuidado para evitar ser interceptados cuando se utiliza adaptadores Bluetooth.

3.3 Voicemail

Los buzones de voz se pueden asignar a personal de la CORPAIRE que necesiten un método para que otros dejen su mensaje cuando ellos no están disponibles. Los buzones de vos deben ser protegidos por un PIN, que nunca debe ser igual a los cuatro últimos dígitos del número de teléfono del buzón de voz.

3.4 Pérdida y Robo

No se deben almacenar en PCDs archivos que contengan datos confidenciales o sensibles, a menos que estos estén protegidos por un método de encriptación. Los costos de reparación debido al mal uso de los equipos o de los servicios deben ser costeados por el empleado, para ello se analizará el caso. El costo de cualquier dispositivo extraviado será responsabilidad del empleado a cargo. La pérdida o robo de los equipos debe ser informado inmediatamente.

3.5 Uso personal

Los PCDs y buzones de voz se asignarán para tareas propias de la CORPAIRE. El uso para actividades personales debe limitarse al uso mínimo u ocasional.

3.6 Seguridad al usar los PCDs

Por regla general, no se debe usar los PCDs para realizar o atender llamadas telefónicas mientras se conduce. Los conductores deben usar los PCDs cuando el vehículo se encuentre parqueado o cuando se encuentren fuera del mismo.

4.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.17 POLÍTICA DE USO DE DISPOSITIVOS DE ALMACENAMIENTO REMOVIBLE

1.0 PROPÓSITO

El propósito de esta política es minimizar el riesgo de pérdida o exposición de información confidencial de la CORPAIRE, así como reducir el riesgo de adquirir infecciones de virus y malware en computadores operados por la corporación durante el uso de dispositivos de almacenamiento removible.

2.0 ALCANCE

Esta política cubre todas los computadores y servidores de la CORPAIRE.

4.0 POLÍTICA

Los empleados de la CORPAIRE sólo puede usar los medios removibles proporcionados por la Corporación en sus equipos de trabajo, los cuales deberán estar protegidos según lo establece la *Política de Antivirus*.

Los medios removibles de la CORPAIRE no pueden ser conectados o usados en computadoras que no son de propiedad o estén arrendadas por la CORPAIRE sin el permiso del Administrador de Seguridad de la Información o del Departamento de Tecnología.

Se debe almacenar información confidencial en medio removibles solo cuando se requiera para el desempeño de sus tareas asignadas o cuando la información sea requerida por agencias gubernamentales.

Cuando la información catalogada como sensible esta almacenada en medios removibles, esta debe ser cifrada de acuerdo a las *Políticas de Cifrado* aceptadas por la CORPAIRE.

5.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.18 POLÍTICA DE CIFRADO ACEPTABLE

1.0 PROPÓSITO

El propósito de esta política es brindar una orientación para el uso del cifrado con algoritmos que han obtenido un reconocimiento público y que han demostrado trabajar eficazmente. Adicionalmente, esta política provee orientación para asegurar el cumplimiento de regulaciones y estándares internacionales.

2.0 ALCANCE

Esta política se aplica a todos los departamentos y empleados de la CORPAIRE.

3.0 POLÍTICA

Los algoritmos como RSA, RC5, IDEA, DES, Blowfish han demostrado su trabajo eficaz y deben ser usados como base para las tecnologías de cifrado, los mismos que forman parte de los mecanismos de cifrado más utilizados actualmente.

La longitud de la clave de un sistema de cifrado simétrico debe ser de por lo menos 128 bits. En este sistema de cifrado tanto el remitente así como el destinatario conocen la clave secreta.

Las claves de los sistema de cifrado asimétrico deben ser de una longitud que proporcione una firmeza equivalente. Si una clave es pública se puede entregar a cualquier persona, la otra clave debe ser privada y el propietario debe guardarla de modo que nadie tenga acceso a ella.

El uso de sistemas de cifrado no autorizados por el Departamento de Tecnología se encuentra prohibido, a menos que sea revisado y aprobado por el Administrador de Seguridad de la Información de la CORPAIRE.

4.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.19 POLÍTICA DE CONTRASEÑAS

1.0 PROPÓSITO

Establecer un estándar para la creación de contraseñas fuertes y seguras, la protección de esas contraseñas, y la frecuencia de cambio.

La selección de una contraseña pobre o débil puede comprometer la red de la CORPAIRE. Todos los empleados con acceso a sistemas computacionales de la CORPAIRE serán responsables de tomar las medidas necesarias para seleccionar y proteger sus contraseñas.

2.0 ALCANCE

El alcance incluye a todo aquel empleado que tiene o es responsable de una cuenta (o cualquier forma de acceso que requiere una contraseña) en cualquier equipo o sistema computacional que tiene acceso a la red de la CORPAIRE.

3.0 POLÍTICA

3.1 General

- Todas las contraseñas de sistema (por ejemplo: Lotus Notes, administrador de ISeries, cuentas de administración, etc.) deben cambiarse en un período de por lo menos un trimestre.
- Todas las contraseñas de sistemas de producción deben ser manejadas a través de la base de datos de contraseñas y administradas por el Departamento de Tecnología.
- Todas las contraseñas de usuario (por ejemplo, el correo electrónico, Web, estación de trabajo, etc.) deben cambiarse cada cuatro meses.
- Las contraseñas no deben insertarse en mensajes de correo electrónico u otras formas de comunicación electrónica.
- Todas las contraseñas de sistema y de usuario deben cumplir las siguientes normas.

3.2 Normas

A. Normas generales para la Construcción de Contraseñas

Todos los usuarios deben asegurarse de seleccionar contraseñas fuertes.

Las contraseñas fuertes tienen las siguientes características:

- Contienen caracteres en mayúsculas y minúsculas (por ejemplo: az, AZ).

- Tiene números, caracteres de puntuación y caracteres especiales (por ejemplo: 0,1,2,3,4,5,7,8,9, ! @ #$% & * () _+ | ~ - = \ {} []: "; '<>?. /).
- Tiene por lo menos quince caracteres alfanuméricos y están en una frase completa (por ejemplo: Ohmy1stubbedmyt0e).
- No es una palabra en cualquier idioma, dialecto, lengua, jerga, etc.
- No se basan en información personal, nombres de familia, etc.

Las contraseñas débiles poseen las siguientes características:

- Contiene menos de quince caracteres.
- Es una palabra encontrada en un diccionario.
- Es una palabra de uso común como:
    - Nombres de familiares, amigos, compañeros, mascotas, etc.
    - Términos y nombres informáticos, comandos, sitios, compañías, hardware, software.
    - Las palabras "CORPAIRE ", “RTV”, "REVISION" o cualquier derivación.
    - Fechas de nacimiento, cumpleaños y otra información personal como direcciones y números telefónicos.
    - Cualquiera palabra deletreada en sentido contrario.
    - Patrones de palabras o de números (aaabbb, aammdd. 123321, etc.)

B. Normas de Protección de Contraseñas

No utilice la misma contraseña de cuentas de la CORPAIRE en otras que no pertenecen a la CORPAIRE (por ejemplo: cuenta personal de ISP, la opción de comercio, beneficios, etc.) Siempre que sea posible, no utilice la misma contraseña para varias cuentas de la CORPAIRE.

No compartir las contraseñas de la CORPAIRE con nadie, incluyendo asistentes administrativos o secretarias. Todas las contraseñas deben ser tratadas como información confidencial de la CORPAIRE.

A continuación una lista de cosas que no se deben hacer:

- No revelar una contraseña por el teléfono a nadie.
- No revelar una contraseña en el texto de un mensaje de correo electrónico.
- No revelar una contraseña al jefe.
- No hablar sobre una contraseña delante de otros.
- No sugiera el formato de una contraseña
- No revelar una contraseña en encuestas o formularios de seguridad.
- No compartir una contraseña con miembros de la familia.
- No revelar una contraseña a los compañeros de trabajo, mientras está de vacaciones.

Si alguien requiere una contraseña, debe referirse a este documento o llamar al Administrador de Seguridad de la Información.

No seleccionar la opción "Recordar Contraseña" de las aplicaciones (por ejemplo: Internet Explorer, Outlook, Messenger).

Cambiar las contraseñas por lo menos una vez cada seis meses (excepto contraseñas de sistema que deben cambiarse trimestralmente).
Si una cuenta o su contraseña es motivo de desconfianza o se sospecha que ha sido revelada, se debe comunicar inmediatamente al Administrador de Seguridad de la Información.

Se debe ejecutar intentos de revelamiento de contraseñas, estos pueden ser ejecutados periódica o aleatoriamente por el Administrador de Seguridad de la Información. Si una contraseña es revelada durante este proceso, se exigirá al propietario de la cuenta que cambie la contraseña.

C. Normas de Desarrollo de Aplicaciones

Los desarrolladores de aplicaciones deben asegurarse que sus aplicaciones contengan las siguientes precauciones de seguridad:

- Deben soportar la autenticación de usuarios individuales, no de grupos.
- No se deben guardar las contraseñas en texto legible o en alguna forma fácilmente reversible.
- Debe proveer la funcionalidad de administrar contraseñas, para que un usuario asuma las funciones de otro, sin tener que conocer las contraseñas de este otro.

D. Uso de Contraseñas y Passphrases para los Usuarios de Acceso Remoto

El acceso remoto a la red de la CORPAIRE debe usar ya sea una autenticación con contraseñas o un sistema con clave pública/privada y con un passphrase fuerte de acceso.

E. Passphrases

Los Passphrases son generalmente usados para la autenticación con clave pública/privada. Un sistema de clave pública/privada determina una relación matemática de seguridad fuerte entre una clave pública que es conocida por todos, y una clave privada que es sólo conocida por el usuario. Sin el passphrase para desbloquear la clave privada, el usuario no podrá obtener acceso.

Lo passphrases están sujetos a las reglas que aplican a las contraseñas.

4.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.20 POLÍTICA DE SEGURIDAD DE SERVIDORES

1.0 PROPÓSITO

El propósito de esta políticas es establecer estándares para la configuración básica de los servidores de la CORPAIRE. La efectiva implementación de esta

política reducirá al mínimo el acceso no autorizado a la tecnología e información de propiedad de la CORPAIRE.

2.0 EL ALCANCE

Esta política aplica a todos los servidores de propiedad de la CORPAIRE, y a los servidores registrados bajo cualquier dominio de la red interna de la CORPAIRE.

Esta política es específicamente para equipos de la red interna de la CORPAIRE. Para garantizar la configuración de equipo externo a la CORPAIRE ubicado en la zona desmilitarizada, referirse a la *Política de Seguridad de la Zona Desmilitarizada DMZ.*

3.0 POLÍTICA

3.1 La propiedad y Responsabilidades

Todos los servidores de producción de la CORPAIRE deben tener un grupo operacional que sea responsable de la administración del sistema. Esta responsabilidad lo tiene el Departamento de Tecnología de la CORPAIRE. Las políticas de configuración de servidores aprobadas deben ser aceptadas y gestionadas por cada grupo operacional, basado en las necesidades del negocio y aprobado por el Departamento de Tecnología. Estos grupos deben supervisar el cumplimiento de la configuración y de ser necesario solicitar la aprobación de las excepciones a la política, esto será revisado y aprobado por el Departamento de Tecnología.

- Los servidores deben ser registrados dentro del sistema de gestión de la CORPAIRE. Se requiere, como mínimo, la siguiente información:
    - Identificar el responsable o contacto y la localización del servidor, además un contacto de reserva.
    - El hardware y la versión del sistema operativo.
    - Aplicaciones y funciones principales, si los posee.
- Debe mantenerse actualizada la información en el sistema de gestión de la corporación.

- Los Cambios de Configuración en los servidores de producción deben seguir los procedimientos de cambio apropiados.

3.2 Normas de Configuración Generales

- La configuración del sistema operativo debe estar alineado a las normas aprobadas por el Departamento de Tecnología.
- Los servicios y aplicaciones que no sean usados deben ser deshabilitados.
- El acceso a servicios debe ser registrado y/o protegido por métodos de control de acceso.
- Se deben instalar los últimos parches de seguridad tan pronto como sean liberados, excepto cuando la instalación interfiera con la funcionalidad de los servicios.
- Se debe evitar el empleo de relaciones de confianza entre sistemas porque pueden ser un riesgo de seguridad.
- No utilizar cuentas con privilegios como root cuando una cuenta sin privilegios pueda ser usada.
- Los servidores deben ser ubicados físicamente en un ambiente cuyo acceso sea controlado y restringido.
- Está prohibido el funcionamiento de los servidores dentro de ambientes que no estén controlados.

3.3 Monitoreo

- Todos los sucesos de seguridad relacionados con sistemas críticos o sensibles deben ser registrados y los rastros de auditorías guardados de la siguiente manera:
    - Todos los incidentes de seguridad se mantendrán mínimo una semana.
    - Los medios de respaldo diarios como cintas, cartuchos, DVD, CD serán conservados durante al menos un mes.
    - Los respaldos semanales serán conservados durante al menos tres meses.
    - Los respaldos mensuales serán conservados mínimo de dos años.

- Los sucesos relacionados con la seguridad serán reportados al Departamento de Tecnología. Se tomarán las medidas correctivas necesarias. Cualquier suceso relacionado con la seguridad incluye, pero no se limita a:
    - Ataques y escaneo de puertos.
    - Evidencias de accesos no autorizados con cuentas privilegiadas.
    - Acontecimientos anómalos que no son relacionados con usos específicos del servidor.

3.4 Auditorías

- Estas serán realizadas dentro de la CORPAIRE por el Departamento de Tecnología.
- Serán manejadas por un grupo interno de auditoría designado por el Departamento de Tecnología, conforme a la *Política de Auditoría*.
- Se debe controlar que las auditorías no causen fallas operacionales o interrupciones en los servicios informáticos.

4.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.21 POLÍTICA DE SEGURIDAD DE ENRUTADORES

1.0 PROPÓSITO

El propósito de esta política es describir la configuración de seguridad mínima requerida para todos los routers y switches conectados a la red de la CORPAIRE.

2.0 ALCANCE

Esta política aplica a todos los routers y switches conectados a la red de la CORPAIRE. Los routers y switches de la DMZ están cubiertos por la *Política de Seguridad de la Zona Desmilitarizada.*

3.0 POLÍTICA

Cada router debe cumplir con los siguientes estándares de configuración:

1. Las cuentas de usuarios locales no deben ser configuradas en el router. Los routers deben usar TACACS+ (sistema de control de acceso mediante control del acceso desde terminales) para autenticación de todos los usuarios.

2. La contraseña de configuración del router debe ser guardada de manera segura y encriptada.

3. Deshabilitar:

a) Envío de broadcast.
b) El ingreso de paquetes al router con direcciones de origen inválidas tales como las especificadas en el documento RFC 1918(direcciones IP privadas).
c) Servicios TCP y UDP que no se justifiquen.
d) Todo tipo de enrutamiento fuente.
e) Todos los servicios Web que estén corriendo en el router.

4. Usar corporativamente cadenas estandarizadas del protocolo SNMP.

5. Las reglas de acceso deben estar dadas en función de las necesidades de la corporación.

6. El router debe estar incluido en el sistema de administración de activos de información de la CORPAIRE con un punto de contacto designado.

7. Cuando se ingresa a la configuración de un router se debe emitir el siguiente texto de seguridad:

ESTÁ TOTALMENTE PROHIBIDO EL ACCESO NO AUTORIZADO A ESTE DISPOSITIVO DE RED

8. Nunca se debe usar el protocolo Telnet para administrar un router. Se debe usar SSH para establecer un canal de comunicación seguro.

4.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.22 POLÍTICA DE RED PRIVADA VIRTUAL (VPN)

1.0 PROPÓSITO

Proporcionar las directrices para las conexiones de acceso remoto VPN con IPSEC o L2TP a la red de la CORPAIRE.

2.0 ALCANCE

Esta política se aplica a todos los usuarios de la red de la CORPAIRE, que pertenezcan o no a la Corporación y que utilizan conexiones VPN.

3.0 POLÍTICA

1. Los usuarios con privilegios de acceso por VPN son responsables de asegurar que no ingresen otros usuarios no autorizados a la red interna de la CORPAIRE.

2. El acceso a la VPN debe ser controlado, se debe usar contraseñas de autentificación. Referirse a las *Políticas de Contraseñas*.

3. Cuando esté activamente conectado en la red, la VPN obligará a todo el tráfico hacia y desde el PC a fluir a través del túnel VPN; el resto del tráfico será dado de baja.

4. No está permitido hacer un doble túnel; sólo se permite una conexión de red.

5. Las VPNs serán configuradas y administradas por los responsables del Departamento de Tecnología.

6. Todos los equipos, incluyendo computadores personales, conectados a la red de la CORPAIRE por medio de una VPN deben usar un software anti-virus actualizado implementado por el Departamento de Tecnología.

7. Los usuarios de la VPN serán desconectados automáticamente de la red luego de diez minutos de inactividad. El usuario debe iniciar nuevamente la sesión para reconectase a la red. No se deben usar comandos ping's u otro tipo de conexión para mantener la comunicación abierta.

8. Solo pueden acceder a la VPN usuarios aprobados por el Departamento de Tecnología.

9. Los usuarios que se conecten con equipos personales usando VPN, deben estas conscientes de que sus equipos son una extensión de la red y como tal están sujetos a las mismas normas que se aplican a los computadores de la CORPAIRE; es decir, sus dispositivos deben estar sujetos a las Políticas de Seguridad del Departamento de Tecnología.

4.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.23 POLÍTICA DE ACCESO REMOTO

1.0 PROPÓSITO

El propósito de esta política es especificar las normas de conexión a la red de la CORPAIRE desde cualquier host remoto. Estas normas se establecen para minimizar el posible riesgo potencial de daños que pueden afectar a la Corporación debido uso no autorizado de sus recursos.

2.0 ALCANCE

Esta política aplica a todas las conexiones de acceso remoto realizadas a la red de la CORPAIRE para obtener servicios de correo electrónico, acceso al Sistema Centralizado de Revisión Técnica Vehicular, aplicaciones de operativos en vía pública, etc.

Las tecnologías de acceso remoto que son cubiertas por esta política incluyen, pero no se limitan a, módems dial-in, frame relay, ISDN, DSL, VPN, SSH, cable módems, etc.

3.0 POLÍTICA

3.1 General

1. Los empleados de la CORPAIRE con privilegios de acceso remoto a la red de la corporación, tienen la responsabilidad de asegurar que su conexión de acceso remoto esté protegida bajo las mismas consideraciones de una conexión local.

2. El acceso a Internet a través de la red de la CORPAIRE para el uso recreativo de los miembros de la familia de un empleado no es permitido, el empleado de la CORPAIRE es responsable de asegurar que su familia no viole ninguna de las políticas, no realice actividades ilegales y no use el acceso para intereses personales. El empleado de la CORPAIRE es responsable de las consecuencias por su mal uso.

3.2 Requisitos

1. El control de seguridad en un acceso remoto será realizado por medio de autenticación de la contraseña o por claves públicas/privadas. Véase la *Política de Contraseñas*.

2. Bajo ninguna circunstancia el empleado de la CORPAIRE proporcionará su cuenta de usuario y contraseña de conexión a cualquier persona incluyendo a los miembros de su familia.

3. Los usuarios de red con privilegios de acceso remoto deben asegurarse que su computadora con la cual se conectan a la Corporación no se conecte al mismo tiempo a otra red, excepto las redes personales que están bajo el control del usuario.

4. Los usuarios de red con privilegios de acceso remoto no deben usar cuentas de correo electrónico gratuitos (Hotmail, Yahoo, Gmail), u otros recursos externos para realizar actividades propias de la CORPAIRE.

5. Todos los dispositivos, incluyendo computadoras personales, conectados a la red por medio de tecnologías de acceso remoto deben usar un software anti-virus actualizado. Las conexiones de terceras partes deben cumplir los requisitos declarados en el *Acuerdo de Terceras Partes*.

6. Las organizaciones o individuos que deseen tener Acceso Remoto no estandarizado a la red deben obtener la aprobación del Departamento de Tecnología.

4.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.24 POLÍTICA DE LA EXTRANET

1.0 PROPÓSITO

El propósito de esta política es describir las normas que deben cumplir las organizaciones de terceros o personas externas que deseen conectarse a la red de la CORPAIRE, con la finalidad de realizar transacciones de negocio con la Corporación.

2.0 ALCANCE

Esta política aplica a las conexiones de terceras partes que requieren el acceso a los recursos no públicos de la CORPAIRE, independientemente de si la

conexión usa un enlace de telecomunicaciones (tales como frame relay o RDSI) o si la conexión es VPN. Los proveedores de servicios de Internet (ISP) que ofrecen acceso a Internet para la CORPAIRE no están bajo esta política.

3.0 POLÍTICA

3.1 Pre-Requisitos

3.1.1 Análisis de la Seguridad

Todas las nuevas conexiones extranet deben pasar por una revisión de seguridad para garantizar el acceso a todos los puntos de conexión de la mejor manera posible, este análisis será realizado por el Departamento de Tecnología.

3.1.2 Acuerdo de terceros en la conexión

Para las conexiones entre terceros y la CORPAIRE se debe firmar un *Acuerdo de Terceras Partes*. Este documento debe ser firmado por el Director de Tecnología de la CORPAIRE y un representante de las terceras partes que esté legalmente facultado.

3.1.3 Punto de contacto

Las terceras partes deben designar una persona que será el punto de contacto (POC) para la conexión Extranet. El POC actuará en nombre de los terceros y permitirá establecer la relación con los ejecutores de esta política.

3.3 Cambio en la Conectividad y Acceso

Toda modificación debe ir acompañada de una justificación válida y está sujeta a un análisis de seguridad. Los cambios se llevarán a cabo a través de un proceso de gestión de cambios. Los terceros son responsables de notificar al administrador de la Extranet sobre toda modificación a fin de que la seguridad y la conectividad también se modifiquen.

3.4 Finalización del Acceso

Cuando ya no es necesario el acceso, las terceras partes deben notificar al administrador de la Extranet.

Se debe realizar una auditoría de la Extranet y de los equipos de seguridad con sus respectivas conexiones, para asegurar que todas las conexiones existentes son necesarias.

Las conexiones que se determinen que ya no están siendo utilizadas se darán por terminadas inmediatamente. En caso de existir un incidente de seguridad o que una conexión vaya a ser eliminada de la Extranet, el administrador notificará los cambios al POC de la entidad externa antes de tomar cualquier acción.

4.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.25 POLÍTICA DE COMUNICACIÓN INALÁMBRICA

1.0 PROPÓSITO

El propósito de esta política es definir las condiciones que deben cumplir los dispositivos de tecnología inalámbrica para conectarse a la red de la CORPAIRE. Sólo los dispositivos inalámbricos que cumplan con las especificaciones de esta política o aquellas excepciones aprobadas por el Departamento de Tecnología tendrán acceso a la red de la CORPAIRE.

2.0 ALCANCE

Esta política se aplica a todos los dispositivos de tecnología inalámbrica que se conectan a la red de la CORPAIRE, incluye pero no se limita a computadoras portátiles, computadoras de escritorio, teléfonos celulares y asistentes personales digitales (PDAs). Esto incluye cualquier forma de dispositivo de comunicación inalámbrico capaz de transmitir paquetes de datos.

Todos los empleados, contratistas, consultores y otros empleados temporales de la CORPAIRE, que deseen conectar un dispositivo inalámbrico a la red de la CORPAIRE deben acatar esta política.

El Departamento de Tecnología de la CORPAIRE deberá aprobar las excepciones a esta política.

3.0 POLÍTICA

3.1 Requisitos Generales de Acceso a la red

Todos los dispositivos inalámbricos que están en algún sitio de la CORPAIRE, que se conecten a la red y que tengan acceso a información clasificada como sensible deben cumplir con los siguientes requisitos:

- El equipo debe ser instalado con el apoyo de un grupo de soporte del Departamento de Tecnología de la CORPAIRE.
- Usar los protocolos de autenticación aprobados por la CORPAIRE.
- Usar los protocolos de cifrado aceptados por la CORPAIRE.
- Mantener un registro de las direcciones MAC para que puedan ser autenticadas y rastreadas.
- No interferir con instalaciones inalámbricas de otras organizaciones.

4.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.26 POLÍTICA DE SEGURIDAD DE REDES LAN INTERNAS

1.0 PROPÓSITO

Establecer los requisitos de seguridad de la información para las redes LAN internas de la CORPAIRE y así asegurar que no se divulgue información confidencial, que las tecnologías de la información no estén comprometidas y que las actividades de la CORPAIRE estén protegidas.

2.0 ALCANCE

Esta política aplica a todos los usuarios y redes LAN de la CORPAIRE. Se deben configurar todos los equipos existentes y futuros que estén bajo el alcance de esta política.

3.0 POLÍTICA

3.1 Responsabilidades de propiedad

1. El Departamento de Tecnología de la CORPAIRE debe tener instalado un firewall entre las redes externas y la red LAN interna de la Corporación.

2. El Departamento de Tecnología se reserva el derecho de interrumpir las conexiones que presenten un riesgo de seguridad a la red.

3. Todas las contraseñas de usuario deben cumplir con la *Política de Contraseñas* de la CORPAIRE. Las cuentas individuales de usuario de cualquier dispositivo deben ser eliminadas cuando el usuario/empleado deje de pertenecer a la corporación.

3.2 Requisitos de la Configuración General

Todo el tráfico de red entre el Internet y la red LAN corporativa debe pasar por un firewall el cual debe estar administrado por el Departamento de Tecnología.

Todos los cambios en las configuraciones originales del cortafuego serán realizados por el Departamento de Tecnología con el propósito de implementar mejoras en lo que se refiera a seguridad.

En la LAN de la CORPAIRE se prohíbe el escaneo de puertos de red y otras actividades similares que afecten o degraden el rendimiento de la red.

4.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.27 POLÍTICA DE RED DE ÁREA LOCAL VIRTUAL (VLAN)

1.0 PROPÓSITO

Proporcionar estándares para conexiones VLAN's al interior de la red de la CORPAIRE.

2.0 ALCANCE

Esta política se aplica a todos los usuarios/empleados que se conectan a la red de la CORPAIRE utilizando una VLAN como medio conexión.

3.0 POLÍTICA

Los usuarios internos que requieran acceder a las facilidades que brinda una VLAN al conectarse a la red de la CORPAIRE deberán solicitar dicho acceso al Departamento de Tecnología.

Es responsabilidad de los usuarios con privilegios de VLAN asegurar que no se permita el acceso a la red interna de la CORPAIRE a otros usuarios que no sean autorizados.

El acceso a la VLAN debe ser controlado, se debe usar contraseñas de autentificación. Referirse a las *Políticas de Contraseñas*.

Las VLANS serán configuradas y administradas por los responsables del Departamento de Tecnología.
Todos los equipos, incluyendo computadores personales, conectados a la red de la CORPAIRE por medio de una VLAN deben usar un software anti-virus actualizado instalado por el Departamento de Tecnología.

Los usuarios de la VLAN serán desconectados automáticamente de la red luego de diez minutos de inactividad. El usuario debe iniciar nuevamente la sesión para reconectase a la red. No se deben usar comandos ping's u otro tipo de conexión para mantener la comunicación abierta.

Solo pueden acceder a la VLAN usuarios aprobados por el Departamento de Tecnología.

Los usuarios que se conecten a la VLAN con equipos personales, deben estas conscientes de que sus equipos son una extensión de la red y como tal están sujetos a las mismas normas que se aplican a los computadores de la CORPAIRE; es decir, sus dispositivos deben estar sujetos a las Políticas de Seguridad del Departamento de Tecnología.

4.0 CUMPLIMIENTO

Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.4.28 POLÍTICA DE ÉTICA

1.0 PROPÓSITO

El propósito de esta publicación sobre ética es enfatizar las expectativas de los empleados y de la ciudadanía, a ser tratados con prácticas comerciales equitativas. Esta política servirá para guiar el comportamiento empresarial para garantizar una conducta ética.

Todos los empleados deben familiarizarse con la normas de ética que sigue esta introducción.

La CORPAIRE está comprometida a proteger a los empleados y así misma de acciones ilegales o perjudiciales realizadas por individuos, consciente o inconscientemente.

La CORPAIRE no tolerará ninguna infracción o irregularidad en cualquier momento. La CORPAIRE tomará las medidas apropiadas para actuar rápidamente en la corrección del problema si el código de ética es roto. Cualquier infracción de este código de ética no será tolerada.

3.0 ALCANCE

Esta política aplica a los empleados, contratistas, consultores, personal temporal, y otros trabajadores de la CORPAIRE, incluyendo a todo el personal afiliado a terceros.

4.0 POLÍTICA

4.1 Compromiso de los Ejecutivos con la Ética

- Los altos ejecutivos en la CORPAIRE deben establecer un buen ejemplo. En cualquier práctica de negocio la honestidad e integridad debe ser prioridad para los ejecutivos.
- Los Ejecutivos deben tener una política de puertas abiertas y bienvenida de sugerencias y preocupaciones de los empleados. Esto permite a los empleados sentirse cómodos discutiendo las cuestiones y alerta a los ejecutivos a preocuparse de la fuerza de trabajo.
- Los Ejecutivos deben revelar cualquier conflicto de intereses respecto a su posición dentro CORPAIRE

4.2 Compromiso de los Empleados con la Ética

- Los empleados de la CORPAIRE tratarán a todos equitativamente, se tendrán respeto mutuo, promoverán un ambiente de equipo y evitarán la intención y aparición de prácticas poco éticas.
- Cada empleado necesita aplicar esfuerzo e inteligencia para mantener el valor de la ética.
- Los empleados deben revelar cualquier conflicto de intereses respecto a su posición dentro de la CORPAIRE
- Los empleados ayudarán a la CORPAIRE a satisfacer a clientes y proveedores, ofreciendo un servicio de calidad y una oportuna respuesta a sus consultas.

4.1 Conciencia de la Corporación

- El promocionar la conducta de ética en las comunicaciones interpersonales de los empleados serán recompensados.

- La CORPAIRE promoverá un ambiente confiable y honesto para reforzar la visión de la ética dentro de la corporación.

4.1 Mantener prácticas de Ética

- La CORPAIRE reforzará la importancia del mensaje de integridad y comenzará en la parte superior. Cada empleado, gerente, director necesita mantener una postura ética y de apoyo al comportamiento ético.
- Los empleados de la CORPAIRE deben favorecer un diálogo abierto, obtener información honesta y tratar a todos equitativamente, con honradez y objetividad.
- La CORPAIRE ha establecido una mejor práctica descubriendo el compromiso, para asegurarnos que el código de ético es entregado a todos los empleados y que las inquietudes relativas al código puedan ser abordadas.

4.1 Comportamiento no Ético

- La CORPAIRE evitará la intención y la aparición de una falta de ética o la práctica de compromiso en las relaciones, acciones y comunicaciones.
- La CORPAIRE no tolerará acoso o discriminación. El uso no autorizado de secretos comerciales & marketing, operativos, financieros, de personal, código fuente, e información técnica integral para el éxito de la corporación no será tolerada.
- La CORPARE no permitirá deshonestidad en cualquier momento y se actuará ética y responsablemente en conformidad con las leyes.
- Los empleados de la CORPAIRE no utilizarán activos corporativos o las relaciones de negocios para uso personal o ganancia.

5.0 CUMPLIMIENTO

- Las infracciones de este código de ética no será tolerada y la CORPAIRE actuará rápidamente para corregir el problema si el código ético está roto.

- Cualquier empleado que viole esta política, puede ser sujeto de acciones disciplinarias, llegando incluso a su despido.

3.5 GLOSARIO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Blogging.

Escribiendo un blog. Un blog (abreviación de weblog) es un diario personal en línea que se actualiza con frecuencia y está destinado al consumo del público en general.

Spam.

Correo electrónico masivo no solicitado y/o no autorizado.

Correo electrónico.

La transmisión electrónica de información usando un protocolo de correo tales como SMTP o IMAP. Algunos clientes de correo electrónico son: Lotus Notes, Eudora, Microsoft Outlook.

Reenvío de correo.

Reenvío de correo electrónico desde una red interna a un punto externo.

Correo tipo cadena.

Reenvío de correo electrónico desde una red interna a un punto externo.

Información sensible.

La información es considerada sensible si esta puede dañar la reputación de la corporación, de los clientes o su posición en el mercado.

Advertencias de correo.

Correo electrónico que contiene advertencias acerca de virus o software malicioso.

Entidad.

Cualquier unidad de negocio, departamento, grupo o terceras partes, interna o externa a la CORPAIRE, responsable del mantenimiento de los activos de la Corporación.

Riesgo.

Aquellos factores que podrían afectar la confidencialidad, la disponibilidad y la integridad de los sistemas y activos claves de información de la CORPAIRE. El Departamento de Tecnología es el responsable de garantizar la integridad, la confidencialidad y la disponibilidad de información crítica y de los activos de computación, minimizando el impacto de procedimientos de seguridad y políticas en la productividad empresarial.

Medidas Adecuadas

Para minimizar el riesgo a la CORPAIRE desde una conexión empresarial externa. El uso de los computadores de la CORPAIRE por los competidores y personal no autorizado debe ser restringido, tal que en el caso de un intento de acceso a la información corporativa de la CORPAIRE, la cantidad de información en riesgo sea mínima.

Configuración de la CORPAIRE a otras conexiones empresariales

Las conexiones deben ser configuradas para permitir que otras empresas vean sólo lo que ellas necesitan ver. Esto implica establecer configuraciones de aplicaciones de y de red que permitan el acceso sólo a lo necesario.

Métodos aprobados de transmisión de archivos electrónicos

Incluye apoyo de clientes FTP y navegadores Web.

Correo Electrónico Aprobado

Incluye todos los sistemas de correo soportados por el Equipo de Apoyo del Departamento de Tecnología. Estos incluyen, pero no necesariamente se limitan al Lotus Notes.

Lenguaje de Computadora.
Un lenguaje usado para generar programas

Credenciales.
Algo que uno sabe (por ejemplo, una contraseña o frase secreta), y/o algo que te identifica (por ejemplo, un nombre de usuario, una huella dactilar, reconocimiento de la voz). Algo que uno sabe y algo que me identifica se presenta para la autenticación.

Derecho.
El nivel de privilegio que ha sido autenticado y autorizado. Los niveles de privilegios a los cuales tiene acceso el recurso.

Hash.
Un número generado algorítmicamente que identifica un dato o su ubicación.

LDAP
Lightweight **D**irectory **A**ccess Protocol. Es un conjunto de protocolos para acceder a los directorios de información.

Servidor.
Para fines de esta política, un servidor es cualquier sistema de computación residente en un centro de datos seguro físicamente adueñado y operado por la CORPAIRE. Además, esto incluye cualquier sistema ejecutando un sistema operativo destinado específicamente como uso de servidor, definido por el Director de Tecnología de la CORPAIRE que tiene acceso a redes seguras. Esto incluye, pero no se limita a, Microsoft Server 2000 y todas sus permutaciones, Microsoft Server 2003 y todas sus permutaciones, cualquier sistema operativo Linux/Unix basados en que los usuarios externos regularmente esperan conectarse.

Malware.
Software diseñado para infiltrar o dañar un sistema informático sin el consentimiento del propietario. Es una mezcla de las palabras "malicioso" y

"software". La expresión es un término generalmente usado por profesionales de la computación y significa una variedad de formas de software o código de programación hostil, intrusivo o molestoso.

Spyware.

Amplia categoría de software diseñado para interceptar o tomar control parcial de un ordenador, operar sin el consentimiento del propietario de esa máquina o usuario legítimo. Mientras que el término tomado literalmente sugiere software que subrepticiamente vigila el usuario, también ha llegado a referirse más ampliamente a software que degrada las operaciones de un ordenador en beneficio de un tercero.

Software Antivirus.

Consiste en programas de computadora que tratan de identificar, impedir y eliminar virus informáticos y otros software maliciosos (malware).

Zona Desmilitarizada (DMZ).

Cualquier red no confiable conectada, pero por separada, a la red de la CORPAIRE mediante un firewall, usado para acceso externo desde el interior de la CORPAIRE. Solo las redes de la DMZ conectadas a la Internet están bajo el alcance de esta política.

Canal Seguro.

Canal que usa cifrado fuerte de acuerdo a las *Políticas de Cifrado Aceptable*. Los canales no cifrados deben usar autenticación de usuario fuerte.

Redes no confiables.

Cualquier firewall de red fuera de la red corporativa para evitar deterioro de los recursos de producción desde el tráfico irregular de red (redes de laboratorio), el acceso no autorizado (redes asociadas, la Internet, etc.), o cualquier otra cosa identificada como una amenaza potencial a esos recursos.

Bluetooth.

Bluetooth es una especificación industrial para redes inalámbricas de área personal (PANs), también conocido como IEEE 802.15.1. Bluetooth proporciona una forma de conectar e intercambiar información entre dispositivos tales como asistentes digitales personales (PDA), y los teléfonos móviles de manera segura, mediante un enlace de radiofrecuencia en la banda ISM de los 2.4 GHz. [5]

Medio Removible.

Dispositivo o medio de comunicación que se puede leer y/o escribir por el usuario final y es capaz de ser trasladado de computadora a computadora sin modificación del ordenador. Esto incluye dispositivos de memoria flash, cámaras, reproductores MP3 y PDAs, discos duros extraíbles, discos ópticos como CD y DVD, discos flexibles y cualquier disco de software comercial y música no dotados por la CORPAIRE

Cifrado.

El cifrado es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.[6]

Sistema de Cifrado Simétrico.

Un método de cifrado en que la misma clave es utilizado para cifrado y descifrado de los datos.

Sistema de Cifrado Asimétrico.

Un método de cifrado en el que son utilizadas dos claves diferentes: una para cifrar y una para descifrar los datos (por ejemplo, la clave pública cifrada).

[5] Fuente: http://es.wikipedia.org/wiki/Bluetooth
[6] Fuente: http://windows.microsoft.com/es-ES/windows-vista/What-is-encryption

Passphrases.

Un passphrase no es lo mismo que una contraseña. Un passphrase es una versión más larga de una contraseña y por consiguiente más seguro. Un passphrase está compuesto de múltiples palabras. Debido a esto, un passphrase es más seguro contra los "ataques de diccionario."

Cuentas de Administración de Aplicaciones.

Cualquier cuenta que sea para la administración de la aplicación. (Ejemplo: Administrador del AS/400, Administrador del Lotus Notes).

RCF 1918.

Request **F**or **C**omments 1918. Asignación de direcciones para Internet privadas. Este documento especifica unas "Mejores Prácticas Actuales", Best Current Practices (BCP), para la comunidad Internet, y solicita su discusión y sugerencias para mejorarlas. La distribución de este memorándum es ilimitada.[7]

Enrutamiento fuente.

Los paquetes IP admiten opcionalmente el enrutamiento fuente, con el que la persona que inicia la conexión TCP puede especificar una ruta explícita hacia él. La máquina destino debe usar la inversa de esa ruta como ruta de retorno, tenga o no sentido, lo que significa que un atacante puede hacerse pasar por cualquier máquina en la que el destino confíe (obligando a que la ruta hacia la máquina real pase por la del atacante). Dado que el enrutamiento fuente es raramente usado, la forma más fácil de defenderse contra esto es deshabilitarlo en el router.[8]

SNMP.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol), en sus distintas versiones, es un conjunto de aplicaciones de gestión de red que emplea los servicios

[7] Fuente: http://www.rfc-es.org/rfc/rfc1918-es.txt
[8] Fuente: http://ants.dif.um.es/~humberto/papers/1997-ati-1.pdf

ofrecidos por TCP/IP, protocolo del mundo UNIX, y que ha llegado a convertirse en un estándar.[9]

Red de Producción.

La "red de producción" es la red utilizada en la actividad diaria de la CORPAIRE. Cualquier red conectada al backbone corporativo, ya sea directamente o indirectamente, la cual carezca de un dispositivo cortafuegos. Cualquier red cuyo deterioro se traduciría en pérdida directa de funcionalidad a los empleados de la CORPAIRE o repercusiones en su capacidad para hacer trabajos.

VPN.

Una red privada virtual o VPN (siglas en inglés de virtual private network), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.[10]

Cable Modem.

Empresas de Cable proveen de acceso a Internet por cable coaxial de Cable TV. Un cable módem acepta este cable coaxial y pueden recibe datos desde Internet sobre 1.5 Mbps. El Cable TV está actualmente disponible sólo en ciertas ciudades.

DSL.

Digital **S**ubscriber **L**ine (DSL) es una forma de conectarse al Internet a alta velocidad, compitiendo con cable módem. DSL trabaja sobre líneas telefónicas estándar y soporta velocidades de datos de más de 2 Mbps en velocidad de bajada (para el usuario) y velocidades lentas de subida (a Internet).

Frame Relay.

Un método de comunicación que gradualmente puede ir desde la velocidad de la RDSI a la velocidad de una línea T1. Frame Relay conecta vía teléfono la red de la empresa.

---

[9] Fuente: http://www.coit.es/publicac/publbit/bit102/quees.htm
[10] Fuente: http://es.wikipedia.org/wiki/Red_privada_virtual

ISDN.

Hay dos sabores de Integrated Services Digital Network o RDSI: BRI y el PRI. El BRI es utilizado para acceso remoto oficina/hogar. BRI tiene dos canales "Portadores" uno de 64kbit (agregado 128kb) y 1 canal D para información de señalización.

Acceso Remoto.

Cualquier acceso a la red de la CORPAIRE mediante un medio o dispositivo de red.

Tunneling.

Acceso simultáneo directo a una red que no es de la CORPAIRE (como Internet, o una red doméstica) desde un dispositivo remoto (PC, PDA, teléfono WAP, etc.) mientras está conectado en la red la CORPAIRE a través de un túnel VPN. VPN Red Privada Virtual (VPN) es un método para acceder a una red remota vía "túnel" a través de Internet.

Extranet.

Una extranet es una red privada que utiliza protocolos de Internet, protocolos de comunicación y probablemente infraestructura pública de comunicación para compartir de forma segura parte de la información u operación propia de una organización con proveedores, compradores, socios, clientes o cualquier otro negocio u organización. Se puede decir en otras palabras que una extranet es parte de la Intranet de una organización que se extiende a usuarios fuera de ella. Usualmente utilizando Internet. La extranet suele tener un acceso semiprivado, para acceder a la extranet de una empresa no necesariamente el usuario ha de ser trabajador de la empresa, pero si tener un vínculo con la entidad. Es por ello que una extranet requiere o necesita un grado de seguridad, para que no pueda acceder cualquier persona. Otra característica de la extranet es que se puede utilizar como una Intranet de colaboración con otras compañías.[11]

[11] Fuente: http://es.wikipedia.org/wiki/Extranet

Circuito.

Para los efectos de esta política, circuito se refiere al método de acceso a la red, ya sea mediante un ISDN tradicional, Frame Relay, etc., o vía tecnologías de cifrado VPN.

Organización Patrocinadora.

La organización de la CORPAIRE quien solicitó que la terceras partes tengan acceso a la CORPAIRE.

Terceras Partes.

Un negocio que no es un formal o parte subsidiaria de la CORPAIRE.

Red de la CORPAIRE.

Una red inalámbrica o cableada incluyendo el interior, exterior, que proporciona conectividad a servicios corporativos.

Conectividad corporativa.

Una conexión que proporcione acceso a una red de la CORPAIRE.

Activos de Información.

La información que es recopilada o producida, el hardware, software, servicios, sistemas, y la tecnología que es necesaria para la obtención, almacenamiento y uso, y asegurando que la información que se reconoce como importante y valiosa para una organización.

Dirección MAC.

La dirección MAC es un número de hardware que identifica de manera única cada nodo en una red y es necesaria para cada puerto o dispositivo que se conecta a la red.

Gateway.

Una Pasarela o puerta de enlace (del inglés Gateway) es un dispositivo, con frecuencia un ordenador, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es

traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.[12]

LAN.

Una red de área local, red local o LAN (del inglés **L**ocal **A**rea **N**etwork) es la interconexión de varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros, con repetidores podría llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de computadoras personales y estaciones de trabajo en oficinas, fábricas, etc. [13]

VLAN.

Una VLAN (acrónimo de Virtual LAN, "Red de Área Local Virtual") es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del Dominio de difusión y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un switch capa 3 y 4). [14]

[12] Fuente: http://es.wikipedia.org/wiki/Gateway_(inform%C3%A1tica)
[13] Fuente: http://es.wikipedia.org/wiki/LAN
[14] Fuente: http://es.wikipedia.org/wiki/VLAN

CAPÍTULO 4

EVALUACIÓN DE LA APLICABILIDAD Y FUNCIONALIDAD

El objetivo de la evaluación de la aplicabilidad y funcionalidad es determinar si es factible aplicar la propuesta de las políticas de seguridad de la información en la CORPAIRE considerando los aspectos legales, económicos, técnicos, organizacionales y operacionales.

4.1 ASPECTOS LEGALES

El Municipio del Distrito Metropolitano de Quito y el Consejo Nacional de Tránsito crearon la Corporación Centros de Revisión y Control Vehicular, como una persona jurídica de derecho privado sin fines de lucro, la misma que fue reconocida mediante Acuerdo Ministerial de Gobierno número 289 de 7 de agosto de 2001.

Por resolución del Directorio de la Corporación, esta se hizo cargo del manejo de la Red de Monitoreo Atmosférico de Quito (REMAQ), con lo cual modificó su nombre y su estatuto ante la misma Cartera de Estado, la que reconoció a CORPAIRE, Corporación para el Mejoramiento del Aire de Quito, mediante Acuerdo 004 de 18 de febrero de 2004.

El 16 de octubre de 2009, el Acta de la Asamblea de la CORPAIRE, dentro de las consideraciones para la disolución de la corporación, contempla el alinear el accionar del municipio al nuevo marco constitucional. Entre otras resoluciones dispuestas esta la siguiente: el mantener las operaciones de la Corporación hasta la culminación del proceso de disolución y liquidación, siempre que éstas no puedan ser trasladadas a un órgano o entidad municipal, sin afectar la continuidad del servicio a la comunidad, por lo tanto se considera como una institución municipal obligada a cumplir con la legislación nacional.

La CORPAIRE requiere la elaboración de Políticas de Seguridad de la Información que le permita validar que la información sea correcta, completa y esté siempre a disposición, además de que sea utilizada únicamente por aquellos que tienen autorización y que los recursos tecnológicos sean aprovechados de manera adecuada y óptima.

Se analizará la aplicabilidad de las Políticas de Seguridad de la Información, haciendo una relación de la CORPAIRE con cada una de las siguientes leyes:

- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos
- Ley Orgánica de Transparencia y Acceso a la Información Pública
- Ley de Propiedad Intelectual
- Constitución del Ecuador

4.1.1 LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS

El objetivo de esta ley es regular los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

La propuesta de Políticas de Seguridad de la Información ayudará a que la CORPAIRE no violente esta ley, específicamente los siguientes artículos:

DE LOS MENSAJES DE DATOS
Artículo 2.- Reconocimiento jurídico de los mensajes de datos
Artículo 3.- Incorporación por remisión
Artículo 4.- Propiedad Intelectual
Artículo 5.- Confidencialidad y reserva
Artículo 6.- Información escrita
Artículo 7.- Información original
Artículo 8.- Conservación de los mensajes de datos
Artículo 9.- Protección de datos

Las políticas que servirán de apoyo para esta ley son las siguientes:

- Política de Uso Adecuado
- Política de Correo Electrónico
- Política de Reenvío Automático de Correo Electrónico
- Política de Retención de Correo Electrónico
- Política de Instalación de Software
- Política de Sensibilidad de la Información
- Política de Contraseñas
- Política de Ética

4.1.2 LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA

Considerando:

Que la Constitución Política de la República, garantiza el derecho a acceder a las fuentes de información, como mecanismo para ejercer la participación democrática respecto del manejo de la cosa pública y la rendición de cuentas a la que están sujetos todos los funcionarios del Estado y demás entidades obligadas por esta Ley;

Que es necesario hacer efectivo el principio de publicidad de los actos, contratos y gestiones de las instituciones del Estado y de aquellas financiadas con recursos públicos o que por su naturaleza sean de interés público;

Que la misma norma constitucional establece que no existirá reserva respecto de informaciones que reposen en archivos públicos, excepto de aquellas que por seguridad nacional no deben ser dadas a conocer.

La propuesta de Políticas de Seguridad de la Información ayudará a que la CORPAIRE no violente esta ley, específicamente en los artículos 3, 5, 6 y 17 que contienen aspectos relativos a la información pública, confidencial, su difusión y resguardo. En estas leyes se aplicarán las Políticas de Uso Adecuado y Sensibilidad de la Información. Los artículos relacionados son:

Art. 3.- Esta Ley es aplicable a los organismos y entidades que conforman el sector público en los términos del artículo 118 de la Constitución Política de la República.

Art. 5.- Información Pública.- Se considera información pública todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las que se refiere esta Ley, contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado.

Art. 6.- Información Confidencial.- Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 (66) y 24 (76) de la Constitución Política de la República.
El uso ilegal que se haga de la información personal, o su divulgación, dará lugar a las acciones legales pertinentes.

No podrá invocarse reserva, cuando se trate de investigaciones que realicen las autoridades públicas competentes, sobre violaciones a derechos de las personas que se encuentren establecidos en la Constitución Política de la República, en las declaraciones, pactos, convenios, instrumentos internacionales y el ordenamiento jurídico interno. Se excepciona el procedimiento establecido en las indagaciones previas.

Art. 17.- De la Información Reservada.- No procede el derecho a acceder a la información pública, exclusivamente en los siguientes casos:

a) Los documentos calificados de manera motivada como reservados por el Consejo de Seguridad Nacional, por razones de defensa nacional, de conformidad con el artículo 81, inciso tercero, de la Constitución Política de la República y que son:

1) Los planes y órdenes de defensa nacional, militar, movilización, de operaciones especiales y de bases e instalaciones militares ante posibles amenazas contra el Estado;

2) Información en el ámbito de la Inteligencia, específicamente los planes, operaciones e informes de Inteligencia y Contrainteligencia militar, siempre que existiera conmoción nacional;

3) La información sobre la ubicación del material bélico cuando esta no entrañe peligro para la población; y,

4) Los fondos de uso reservado exclusivamente destinados para fines de la defensa nacional; y,

b) Las informaciones expresamente establecidas como reservadas en leyes vigentes.

4.1.3 LEY PROPIEDAD INTELECTUAL

La Ley de Propiedad Intelectual (LPInt.), publicada en el Registro Oficial N°320 del 19 de Mayo de 1998, nace con el objetivo de brindar por parte del Estado una adecuada protección de los derechos intelectuales y asumir la defensa de los mismos, como un elemento imprescindible para el desarrollo tecnológico y económico del país.

El organismo nacional responsable por la difusión, y aplicación de las leyes de la Propiedad Intelectual en el Ecuador es el INSTITUTO ECUATORIANO DE PROPIEDAD INTELECTUAL (IEPI), el mismo que cuenta con oficinas en Quito, Guayaquil y Cuenca. Es una persona jurídica de derecho público, con patrimonio propio, autonomía administrativa, económica, financiera, y operativa, con sede en la ciudad de Quito.

La CORPAIRE tiene registrado en el IEPI el Sistema Centralizado de Revisión Técnica Vehicular (SC-RTV). Todos los archivos, tablas y programas para

gestionar estas entidades, son creados por el personal técnico del Departamento de Tecnología de la CORPAIRE, por tal motivo fue necesario realizar el trámite respectivo para cumplir esta ley. El artículo que cumplió la corporación es:

Art. 28.- Los programas de ordenador se consideran obras literarias y se protegen como tales. Dicha protección se otorga independientemente de que hayan sido incorporados en un ordenador y cualquiera sea la forma en que estén expresados, ya sea en forma legible por el hombre (código fuente) o en forma legible por máquina (código objeto), ya sean programas operativos y programas aplicativos, incluyendo diagramas de flujo, planos, manuales de uso, y en general, aquellos elementos que conformen la estructura, secuencia y organización del programa.

La propuesta de Políticas de Seguridad de la Información, no posee una política específica que valide esta ley; sin embargo se puede citar la Política de Sensibilidad de la Información como aquella que sea de apoyo para el cumplimiento de esta ley.

4.1.4 CONSTITUCIÓN DEL ECUADOR

Capítulo Sexto

Derechos de Libertad

Art 66. Se reconoce y garantiza a las personas:

27. El derecho a vivir en un ambiente sano, ecológicamente equilibrado, libre de contaminación y en armonía con la naturaleza.

La misión de la CORPAIRE es mejorar la calidad del aire de Quito. Esto se logra mediante el proceso de la Revisión Técnica Vehicular, que a través de herramientas de apoyo como son el instructivo de revisión vehicular y el Sistema Centralizado de Revisión Técnica Vehicular (SC-RTV) hacen posible que la calidad del aire y la contaminación ambiental disminuyan.

El uso de las Tecnologías de la Información y Comunicaciones por parte de la CORPAIRE, hacen posible que las operaciones y actividades de la institución se desarrollen de la manera más técnica y eficiente. La propuesta de Políticas de Seguridad de la Información fortalecerá el uso correcto y adecuado de aquellas tecnologías.

Es así como la misión de la CORPAIRE no se verá afectada y en consecuencia el derecho a vivir en un ambiente sano, ecológicamente equilibrado, libre de contaminación y en armonía con la naturaleza.

Conclusión:
En vista de que la mayoría de las Políticas de Seguridad de la Información son de soporte para el cumplimiento de las leyes citadas, se concluye que estas políticas son aplicables en el aspecto legal.

4.2 ASPECTOS ECONÓMICOS

A continuación se presenta un análisis que permite evaluar la factibilidad de la implantación de las Políticas de Seguridad de la Información, tomando en cuenta los aspectos económicos.

4.2.1 COSTOS DE IMPLEMENTACIÓN

Costos de Personal involucrado.

Para identificar los costos respecto al esfuerzo humano que se necesitará para la implementación de esta propuesta se ha tomado en cuenta los siguientes aspectos:

- Horas laborables. La jornada laboral en la CORPAIRE es de ocho (8) horas diarias, es decir 160 horas mensuales.
- Valor promedio de ingresos por cada nivel remunerativo involucrado en la implementación.
    - o Directivo USD $ 2.500,00 (15,63 / hora)
    - o Técnico USD $ 1.600,00 (10,00 / hora)

Tomando en cuenta que cada una de las personas involucradas en la implementación de este proyecto dedique mínimo una (1) hora diaria de su jornada laboral, el total de horas al mes sería de veinte (20) y al año doscientos cuarenta (240). Con este factor y considerando los aspectos anteriormente mencionados, se muestra la tabla 4.1 con el costo anual del personal involucrado.

CANT.	PERSONAL	NIVEL	VALOR/ HORA	COSTO ANUAL
1	Director de la CORPAIRE	Directivo	15,63	3.751,20
1	Director de Tecnología(Jefe del Proyecto)	Directivo	15,63	3.751,20
1	Encargado del Proyecto	Técnico	10,00	2.400,00
1	Apoyo Informático	Técnico	10,00	2.400,00
COSTO TOTAL DE LA IMPLEMENTACION				**12.302,40**

Tabla 4.1 Costos estimados del personal involucrado en la implementación.

Costos de Mantenimiento de las Políticas.

En la figura 4.1 se presenta un diagrama de la planificación y sus costos de la fase de mantenimiento de las Políticas de Seguridad de la Información, la cual busca concienciar a los empleados de la CORPAIRE de la importancia de las políticas, las cuales deberán ser monitoreadas para validar su efectividad, garantizar su cumplimiento y, de ser necesario, corregirlas o actualizarlas.

Actividades	2011									2012		
	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	ENE	FEB	MAR
Concienciación			Apoyo informático									
Monitoreo					Encargado del Proyecto							
Garantía de Cumplimiento						Jefe de Proyecto						
Mantenimiento								Encargado del Proyecto				

ETAPA	HORAS	COSTO/HORA	TOTAL
Concienciación	40	10,00	400,00
Monitoreo	40	10,00	400,00
Garantía de Cumplimiento	20	15,63	312,60
Mantenimiento	40	10,00	400,00
Costo Total de Mantenimiento			**1.512,60**

Figura 4.1 Planificación y Costos de la Fase de Mantenimiento

Adicionalmente a estos costos, es necesario identificar otros costos del proyecto, tal como se muestra en la tabla 4.2.

DESCRIPCION	VALOR
Costos de la Fase de Mantenimiento	1.512,60
Costos de Difusión	500,00
Costos de Administración	800,00
Otros costos	700,00
TOTAL COSTOS	**3.512,60**

Tabla 4.2 Total Costo de Mantenimiento

El ciclo de vida del proyecto será de mediano plazo, tres años, durante este período se identifican los costos de mantenimiento tomando en cuenta el índice de inflación anual del año 2010 proporcionado por el Banco Central del Ecuador y que es 3.33 %, tal como se muestra en la tabla 4.3.

	CICLO DE VIDA DEL PROYECTO			
AÑO	0	1	2	3
Costo de Mantenimiento	0,00	3.512,60	3.629,57	3.750,43

Tabla 4.3 Proyección de Costos de Mantenimiento

4.2.2 PROYECCIÓN DE COSTOS DURANTE LA VIDA UTIL DEL PROYECTO

Los factores de entrada para la proyección de costos durante la vida útil de proyecto son:

- Costo de Hardware y Software. Tomado del Presupuesto para la adquisición de equipos de seguridad, según la planificación Operativa Anual (POA) de la CORPAIRE. Véase subcapítulo 4.3.3.
- Costo de recurso humano involucrado para Implementación de las Políticas
- Índice de inflación de costos de mantenimiento
- Costo de Mantenimiento de las Políticas

AÑO	Hardware y Software	Recurso Humano	Indice Inflación	Costo Mantenimiento Políticas	Costos Totales
0	35.000,00	12.302,40	0,00	0,00	47.302,40
1	0,00	0,00	0,00	3.512,60	3.512,60
2	0,00	0,00	0,03	3.629,57	3.629,60
3	0,00	0,00	0,03	3.750,43	3.750,47
					58.195,07

Tabla 4.4 Costos estimados

4.2.3 BENEFICIOS

Al finalizar la implementación de las Políticas de Seguridad de la Información, se deberá identificar los beneficios que genera este proceso. Los beneficios que la CORPAIRE puede obtener con la implementación de este proyecto son los siguientes:

- Mejora de la calidad de servicio al usuario externo e interno.
- Mejor uso y aprovechamiento de los activos de información y recursos de TI de la corporación.
- Mejora de la confidencialidad, integridad y disponibilidad de los activos de información.

- Mayor eficiencia de parte del Departamento de Tecnología a la hora de resolver requerimientos respecto a seguridades de la información.
- Mejora en la gestión y control de los activos de información.
- Reducción de los riesgos inherentes a la seguridad de la información.
- Mejora de la imagen de la CORPAIRE.
- Mejor reacción a incidentes de seguridad de la información.
- Cuantificación de los posibles daños por ataques a la seguridad de la información.
- Concientización del personal de la CORPAIRE sobre la importancia de la seguridad de la información.
- Aumento de la confianza de parte de terceros.

El objetivo general de estos beneficios es mejorar la entrega de servicios y la productividad de la CORPAIRE, a continuación se cuantificará a los mismos.

4.2.4 CUANTIFICACIÓN DE BENEFICIOS

El cuantificar los beneficios puede ser relativo, ya que se toma en cuenta posibilidades de que suceda un determinado evento u otro. Por lo tanto la manera de cuantificar los beneficios se hace tomando en cuenta la probabilidad de dejar de percibir dichos beneficios si no se realiza la inversión.

Para aclarar este tema es necesario definir costo de oportunidad.

Costo de Oportunidad.

En gestión y finanzas el costo de oportunidad de una inversión es el costo de la *no realización* de la misma.

Para cuantificar los beneficios de esta propuesta, se tomarán en cuenta valores estimados respecto a la productividad de la CORPAIRE y costo de servicio de Internet.

Productividad laboral

La productividad es el rendimiento o eficiencia de la actividad productiva de las personas expresada por la correlación entre el gasto de trabajo y la cantidad de bienes producidos en una unidad de tiempo.

La tecnología es un factor que se debe considerar cuando se desea mejorar la productividad de una organización. Por ejemplo la tecnología permite brindar una mejor atención al cliente y mejorar la calidad del servicio, ayuda a reducir costos, en si a ser más productivos.

Empero la tecnología puede ser usada por los empleados para actividades no relacionadas con su trabajo, como leer correos electrónicos personales, descargar música o videos, realizar compras en línea. Esto conlleva a que el computador se constituye en una herramienta que va a reducir la productividad.

Según datos proporcionados por el Departamento de Tecnología de la CORPAIRE, el 94% de los empleados tienen acceso a los servicios de Internet y correo electrónico; y lo usan para mejorar su productividad, el 3% usan estos servicios para actividades no relacionadas con su trabajo reduciendo así su productividad y el 3% restante no tiene acceso a estos servicios.

Las Tecnologías de la Información (TI) en la corporación es de gran impacto en la calidad del trabajo, un gran porcentaje de los empleados de la CORPAIRE usan TI para mejorar su productividad, ya que se cuenta con un buen proveedor de servicios de Internet así como de equipos, los cuales proveen de un buen ancho de banda.

La jornada laboral en la CORPAIRE es de 8 horas diarias, es decir; 40 horas semanales, en consecuencia 160 horas mensuales. Sin embargo, como en todas las organizaciones, existe un tiempo no productivo de los empleados. Este tiempo lo usan para actividades como refrigerio, uso inadecuado de teléfono fijo, uso de celular, tiempo entre comidas, cafés, reuniones no autorizadas en salas o pasillos, etc. La CORPAIRE considera que todos estos

tiempos suman una hora diaria de actividades no productivas y representan un 12,50% de la jornada laboral.

La CORPAIRE maneja anualmente un presupuesto de USD $950.000,00 para el pago de sueldos a sus empleados. Si se aplica el 12,50% sobre el monto anterior, la CORPAIRE está pagando anualmente USD $118.750,00 por horas no productivas, el mismo que puede ser ahorrado y considerado como beneficio.

Servicio de Internet

La CORPAIRE maneja un presupuesto anual de USD $ 20.000,00 para pago a proveedores de servicio de Internet, según datos proporcionado por el Departamento de Tecnología de la CORPAIRE el 20% del tráfico de la red corporativa es destinada a actividades no productivas, es decir los recursos de TI están siendo mal utilizados. Si se elimina este 20%, el costo de oportunidad anual sería USD $ 4.000,00.

A continuación se presenta la tabla 4.5 la cual presenta un resumen de beneficios cuantificados de forma anual y se determina el costo total anual del beneficio que es de USD $122.750,00.

PARAMETRO	BENEFICIO ANUAL
Productividad laboral	118.750,00
Servicio de Internet	4.000,00
TOTAL	**122.750,00**

Tabla 4.5 Costo de beneficios

4.2.5 PROYECCIÓN DE BENEFICIOS DURANTE LA VIDA UTIL DEL PROYECTO

En función del costo total anual del beneficio, se obtendrá una variación progresiva del 33% anual durante los tres años de duración del proyecto. Véase la tabla 4.6.

AÑO	Beneficio esperado	Porcentaje de variación	Beneficio Real
0	0,00	0,00%	0,00
1	122.750,00	33,00%	40.507,50
2	122.750,00	67,00%	82.242,50
3	122.750,00	100,00%	122.750,00
			245.500,00

Tabla 4.6 Beneficios estimados en USD durante el proyecto

La Figura 4.2 permite visualizar una proyección de la relación costo-beneficio a lo largo de la vida útil del proyecto.

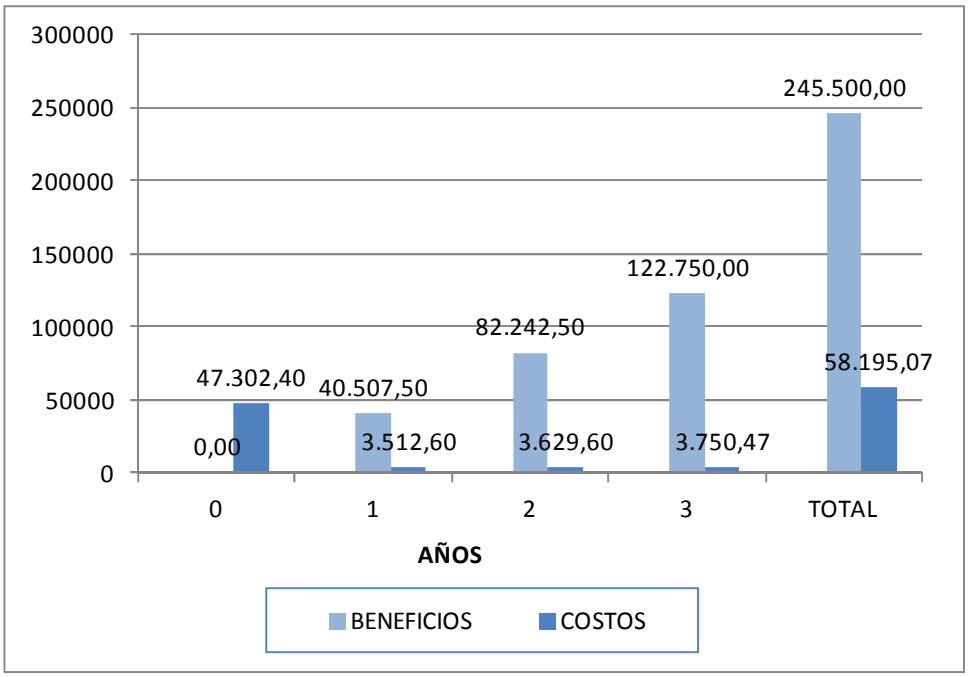

Figura 4.2 Relación Costo – Beneficio del Proyecto

4.2.6 CÁLCULO DE VARIABLES FINANCIERAS (VAN, TIR, PRI)

Los valores de Flujo Neto de Caja (FNC) y la Sumatoria, que se pueden visualizar en la tabla 4.7, permiten realizar el cálculo de las variables financieras, las cuales permitirán tomar una decisión respecto de la factibilidad económica de este proyecto.

Año	Costos	Beneficios	Flujo Neto de Caja (FNC)	Sumatoria (SFNC)
0	47.302,40	0,00	-47.302,40	-47.302,40
1	3.512,60	40.507,50	36.994,90	-10.307,50
2	3.629,60	82.242,50	78.612,90	68.305,40
3	3.750,47	122.750,00	118.999,53	187.304,93

Tabla 4.7 Flujo de Caja del Proyecto

El FNC de cada año permite realizar el cálculo de las variables financieras, tales como el Valor Actual Neto, Tasa Interna de Retorno usando las funciones financieras VNA y TIR respectivamente del Microsoft Excel, con una tasa de interés activa efectiva del 10.21%.[15]

Valor Actual Neto (VAN)	139.883,23
Tasa Interna de Retorno (TIR)	112%

Tabla 4.8 Variables Financieras del Proyecto

El Período de Recuperación de la Inversión (PRI) se calcula con la siguiente fórmula:

PRI = t2 + | SFNC2 | * (t3 – t2) / (| SFNC2 | + | SFNC3 |)
PRI = 1,13 años

[15] Tasa BCE Abril 2011

4.2.7 ANÁLISIS DE VARIABLES FINANCIERAS

VALOR ACTUAL NETO (VAN)

El VAN es un procedimiento que permite calcular el valor presente de un determinado número de flujos de caja futuros, originados por una inversión. La regla para la toma de decisión de aceptar o rechazar un proyecto es la siguiente:

CONDICION	DECISION
VAN > 0	Aceptar proyecto
VAN < 0	Rechazar proyecto
VAN = 0	Aceptar o Rechazar

El VAN de este proyecto es de USD $ 139.883,23. Si se acepta la realización de este proyecto usando la regla de toma de decisiones, se garantiza la recuperación de la inversión ya que el VAN es mayor a cero.

TASA INTERNA DE RETORNO (TIR)

Este indicador mide la rentabilidad en términos porcentuales y se puede definir como el porcentaje de ganancia en una inversión. Si **r** es la tasa de interés activa efectiva, entonces la regla para la toma de decisión de aceptar o rechazar un proyecto es la siguiente:

CONDICION	DECISION
TIR > r	Aceptar proyecto

La Tasa Interna de Retorno es del 112% que es mayor a la tasa de interés activa efectiva (r) del 10.21%.

PERÍODO DE RECUPERACIÓN DE LA INVERSIÓN

Mide la rentabilidad del proyecto en términos de tiempo. Si **p** es el tiempo de vida del proyecto, entonces la regla para la toma de decisión de aceptar o rechazar un proyecto es la siguiente:

CONDICION	**DECISION**
PRI < p	Aceptar proyecto

El Período de Recuperación de la Inversión de este proyecto es de 1,13 años y es menor al tiempo de vida del proyecto (p) que es de 3 años.

Conclusión:
Las variables financieras demuestran que este proyecto es factible y que de no ejecutarlo, se dejaría de percibir los beneficios planteados.

4.3 ASPECTOS TÉCNICOS

La factibilidad de aplicabilidad de esta propuesta de políticas en función de los aspectos técnicos, se valida al realizar los pasos previos al proceso de adquisición tales como:

- Diseñar un esquema de seguridad
- Determinar las especificaciones técnicas mínimas de los equipos que se van adquirir/licitar.

Sin embargo la CORPAIRE para adquirir los equipos debe seguir los siguientes pasos:

1. Diseñar un esquema de seguridad.
2. Determinar las especificaciones técnicas mínimas de los equipos que se van adquirir/licitar.
3. Presupuesto.
4. Iniciar el proceso de adquisición/licitación.

4.3.1 ESQUEMA DE SEGURIDAD

Se propone el siguiente esquema de seguridad, en base al mismo se realizará la adquisición de los equipos necesarios. Véase la figura 4.1

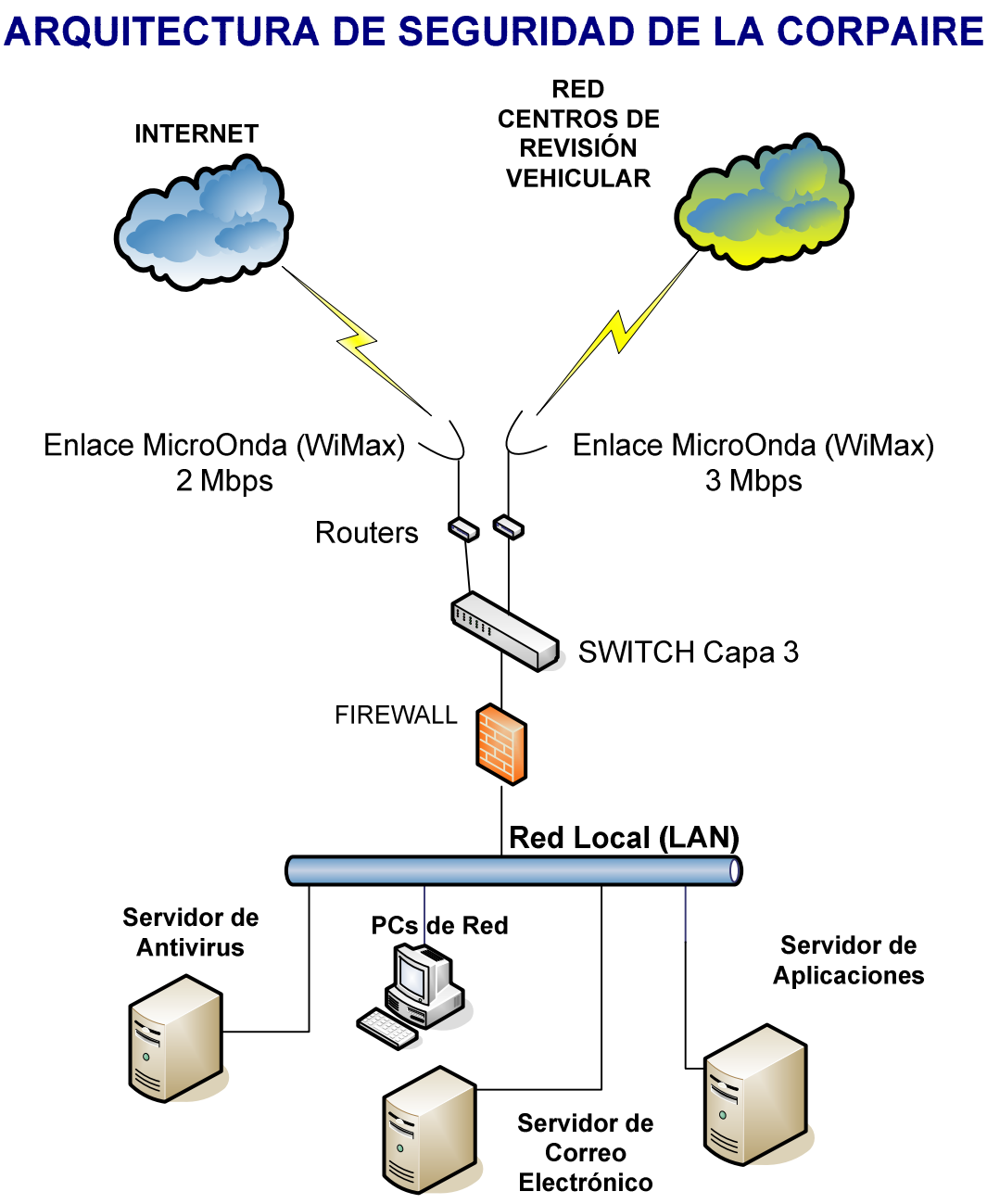

Figura 4.3 Esquema de Seguridad de la CORPAIRE

4.3.2 ESPECIFICACIONES TÉCNICAS MÍNIMAS DE LOS EQUIPOS DE SEGURIDAD

1. SWITCH

- Capa 3
- 24 puertos 10/100 Base *T*, 1 puerto de administración RJ-45, 1 puerto de consola RJ-45 puertos SFP.
- 128 MB en memoria RAM
- Métodos de autenticación: Kerberos, RADIUS, TACACS+, SSH2
- 326.100 horas de vida promedio del equipo
- Modo de comunicación: Half-duplex, full dúplex
- Protocolos: Ruteo IP, soporte: DHCP, ARP, VLAN, IGMP snooping, IP V6.
- Tamaño de la tabla de direcciones MAC: 12 K entradas
- Protocolos de Administración Remota: SNMP v1 / v2 / v3, RMON v1 / v2, Telnet
- Power over Ethernet: soportado
- Protocolos de ruteo: OSPF, IGRP, BGP-4, RIP, v1/v2, EIGRP, HSPR, DVMRP, PIM-SM, ruteo estático, PIM-DM, IGMP v3
- Estándares compatibles: 802.3, 802.3u, 802.3z, 802.1D, 802.1Q, 802.3ab, 802.1p, 802.3x, 802.3ad (LACP), 802.1w, 802.1x, 802.1s
- Garantía

2. FIREWALL

- Filtrado de Contenidos web
- Rendimiento IPS: 60 Mbps
- Sesiones IPS concurrentes: 128.000
- Filtros de ataques: 2.300 + filtros de ataques contra spyware, gusanos, virus, troyanos, phishing, amenazas de VoIP, DoS, P2P, IM
- Actualizaciones automática de filtros de ataque
- Rendimiento: 100 Mbps
- Políticas: mínimo 500
- Zonas de seguridad: mínimo 32
- 1.000 de sesiones de clientes concurrentes en conexiones VPN

- Protocolo soportados para VPN: IPSec nativo, L2TP / PISec, PPTP / MPPE
- Filtrado de Antispam
- Interfaces de Red LAN 10/100/1000 BASE-TX, 1 puerto DMZ 10/100 BASE-TX y 1 puerto WAN 10/100 Mbps BASE-TX
- Puerto serial RJ-45
- Administración de la consola de configuración tipo web
- Alta disponibilidad
- Autenticación de usuarios
- Garantía

3. SOFTWARE ANTIVIRUS PARA LA CORPAIRE

- El antivirus debe haber pasado las pruebas de virus boletín, por lo menos en los siguientes sistemas operativos: Windows XP, Windows 2003 Server, Windows Vista, Windows 2007.
- Licencia para 80 clientes
- Soporte técnico.
- El tipo de licencia del antivirus debe ser Suite Integral, que cuente con una sola consola de administración central instalable sobre plataforma Windows 2003 Server, que permita el control y monitoreo de las computadoras personales conectadas a la red de la CORPAIRE.

4.3.3 PRESUPUESTO PARA LA ADQUISICIÓN DE LOS EQUIPOS DE SEGURIDAD

Según la Planificación Operativa Anual (POA) de la CORPAIRE, el presupuesto asignado al Departamento de Tecnología es de aproximadamente USD 350.000, de los cuales se ha destinado un monto de USD 35.000 para la adquisición de los equipos anteriormente mencionados. Dentro de este presupuesto se considera la adquisición de:

1 Switch

1 Firewall

1 Software Antivirus

4.3.4 PROCESO DE ADQUISICIÓN/LICITACIÓN

Todo este proceso esta soportado y debe ser ingresado en el sistema informático vía web http://www.compraspublicas.gov.ec del Instituto Nacional de Contratación Pública (INCOP). La CORPAIRE debe ingresar el RUC, usuario y contraseña para ingresar en este sistema.

El proceso de adquisición inicia con la publicación de las bases en el portal del INCOP. Las empresas calificadas podrán acceder a estas bases y enviar sus ofertas.

La compra puede ser:

1. Directa si el monto va desde USD $0,00 hasta USD $200,00
2. Por menor cuantía si el monto va desde USD $201,00 a USD $500,00
3. Menor cuantía con orden de compra si el monto va desde USD $501,00 hasta 3500 dólares, y
4. Subasta inversa si el monto es de USD $3501,00 dólares o superior

Conclusión:

Se concluye que este proyecto es factible en el aspecto técnico, ya que existe el presupuesto necesario para la compra de los dispositivos de seguridad

4.4 ASPECTOS ORGANIZACIONALES

El objetivo de los aspectos organizacionales es determinar las personas involucradas en el desarrollo de las Políticas de Seguridad en la CORPAIRE estableciendo un comité se seguridad y determinar los responsables en cada etapa del ciclo de vida de las políticas.

4.4.1 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información es el ente encargado de llevar a cabo la ejecución del proceso de desarrollo de las políticas de seguridad durante el ciclo de vida de estas políticas. Este comité deberá ser integrado por técnicos del Departamento de Tecnología de la CORPAIRE, ya que este departamento es responsable de la administración de los recursos de TI de la corporación y quienes durante todo el proceso deberán ser los responsables directos de la ejecución de este proyecto y posteriormente de su monitoreo y mantenimiento.

Miembros

El Comité de Seguridad de la Información deberá estar conformado por los siguientes miembros:

- Director Ejecutivo de la CORPAIRE
- Asesor Jurídico
- Director de Tecnología
- Oficial o Administrador de Seguridades
- Miembros del Departamento de Tecnología

Funciones

1. Revisar y presentar al Directorio de la CORPAIRE la propuesta de Políticas de Seguridad de la Información para su revisión y aprobación.

2. Llevar el proceso de implantación de las Políticas de Seguridad de la Información en la CORPAIRE.

3. Analizar y aprobar metodologías y procesos específicos relacionados a la seguridad de la información.

4. Evaluar y coordinar la implementación de controles específicos en nuevos sistemas o procesos respecto a la seguridad de la información.

5. Promover la difusión de las Políticas de Seguridad de la Información dentro de la corporación.

4.4.2 RESPONSABLES DURANTE EL CICLO DE VIDA DE LAS POLÍTICAS

Para asignar los responsables en cada etapa del ciclo de vida de las políticas, se tomará en cuenta los roles definidos en el subcapítulo acápite 4.5 Aspectos Operativos.

A continuación se exponen cada una de las etapas del ciclo de vida, siendo la etapa de creación la única que se aplica en este documento; las otras están fuera del alcance de este proyecto de tesis.

Etapa de Creación

El responsable de esta etapa es el autor de este proyecto de tesis. Sin embargo es el Director de Tecnología el responsable directo del proyecto dentro de la CORPAIRE, y se le denominará:

- Encargado del Proyecto

Etapa de Revisión

- Comité de Seguridad de la Información.

Etapa de Aprobación

- Director Ejecutivo
- Asesor Jurídico
- Directorio de la CORPAIRE

Etapa de Comunicación

- Encargado del Proyecto

Etapa de Cumplimiento

En esta etapa se requiere de personas con responsabilidades de supervisión y toma de decisiones en la corporación:

- Director Ejecutivo
- Directores o Jefes de Área

Etapa de Excepciones

- Comité de Seguridad de la Información

Etapa de Concienciación

- Encargado del Proyecto.

Etapa de Monitoreo

En esta etapa se requiere de personas con responsabilidades de supervisión:

- Director Ejecutivo
- Directores o Jefes de Área

Etapa de Garantía de cumplimiento

En esta etapa se requiere de personas con responsabilidades de supervisión:

- Director Ejecutivo
- Directores o Jefes de Área

Etapa de Mantenimiento

- Comité de Seguridad de la Información.

Etapa de Retiro

- Comité de Seguridad de la Información

Conclusión:

Es factible la aplicabilidad de esta propuesta en el aspecto organizacional puesto que la CORPAIRE dispone del personal necesario para el desarrollo de la propuesta. Además las horas que el personal dedique a la ejecución del proyecto están consideradas dentro del horario normal de trabajo por ende no representan un gasto extra.

La participación de los niveles directivos de la CORPAIRE es muy importante para avalar la implementación de las políticas.

4.5 ASPECTOS OPERATIVOS

Los roles a ser desempeñados por el recurso humano de la CORPAIRE, son necesarios para establecer una planificación inicial en el caso de una implementación. A continuación se presenta una descripción del perfil de cada rol.

Director Ejecutivo: Autoridad de la CORPAIRE y miembro del Directorio, responsable de la aprobación de las políticas. Como la corporación está en proceso de liquidación el rol lo desempeñará el Liquidador de la CORPAIRE, que tiene las mismas funciones y responsabilidades.

Directorio de la CORPAIRE: Organismo de la CORPAIRE responsable de la aprobación de las políticas que rigen a la institución.

El Directorio de la CORPAIRE está conformado por: el Alcalde Metropolitano de Quito, el Comandante General de la Policía Nacional, el Secretario de

Ambiente, el Subsecretario de Transportes, el Director Nacional de Tránsito, el Rector de la Escuela Politécnica Nacional y el Director Ejecutivo de Fundación Natura.

Asesor Jurídico: Persona con la autoridad requerida, responsable del asesoramiento, análisis y cumplimiento legal de las políticas.

Encargado del Proyecto: Persona(s) de la corporación que bajo la responsabilidad del Departamento de Tecnología será el encargado de la implantación de las Políticas de Seguridad de la Información en la CORPAIRE.

Directores o Jefes de Área: Personas representantes de los departamentos o áreas de la CORPAIRE, encargados de la difusión, cumplimiento, monitoreo, análisis y definición de las políticas.

Conclusión:

Se concluye que es factible la aplicabilidad de esta propuesta en el aspecto operativo puesto que la CORPAIRE posee el recurso humano necesario y cuenta con el apoyo de los directivos para el desempeño de los diferentes roles necesarios para la realización del presente proyecto.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Para apoyar los principios básico de seguridad de la información, como son la integridad, confidencialidad y disponibilidad es necesario la creación de las Políticas de Seguridad de la Información.

- Debido a requerimientos operacionales y regulaciones técnicas de la CORPAIRE, existe la necesidad de crear las Políticas de Seguridad de la Información,

- La identificación del conocimiento organizacional representa una clave para el desarrollo de las Políticas de Seguridad de la Información aplicables a la realidad de la corporación.

- La CORPAIRE es una institución de carácter privado sin fines de lucro pero alineadas a la normativa del Municipio de Quito, la misma que debe cumplir con la legislación ecuatoriana vigente y los tratados internacionales.

- La participación de todos los empleados de la CORPAIRE es imperiosa para la ejecución y cumplimiento de estas políticas.

- La ISO/IEC 27005 es una norma que proporciona directrices para la Gestión del Riesgo de Seguridad de la Información en una organización. Sin embargo, esta norma no proporciona ninguna metodología específica para el análisis y la gestión del riesgo de la seguridad de la información.

5.2 RECOMENDACIONES

- Se recomienda realizar una evaluación de las Políticas de Seguridad de la Información con una periodicidad de un año.

- Debido a que la información es muy importante para la organización, se recomienda que la corporación capacite a su personal técnico en todo lo referente a las normas y marcos de trabajo de Seguridad de la Información, y no verlo como un gasto sino más bien como una inversión, puesto que los beneficios obtenidos sobrepasan fácilmente a los costos de inversión.

- En caso de aprobarse la implementación de estas Políticas de Seguridad de la Información en la CORPAIRE, se recomienda que estas se constituyan en documentos públicos de la corporación.

- Se debe comunicar a los empleados sobre los beneficios y ventajas que se obtendrán luego de la implementación de estas políticas. De igual manera se debe concienciar sobre el cumplimiento y sanciones descritas en las políticas.

BIBLIOGRAFÍA

1) CORPAIRE. Página web de la Corpaire. Internet: http://www.corpaire.org/siteCorpaire/quesomos.jsp Acceso: 2010-01-05

2) ISO 27000. El portal de ISO 27001 en Español. Internet. http://www.iso27000.es/ Acceso: 2010-02-23

3) ISO. ISO-IECJTC1-SC27_N8923_FCD_27005_20100602[1]. Edición en Inglés. Año 2008.

4) WIKIPEDIA. Sans Institute. Interner: http://es.wikipedia.org/wiki/SANS Acceso: 2010-0215

5) SANS INSTITUTE. Information Security Policy Templates. Internet. http://www.sans.org/security-resources/policies/ Acceso: 2010-02-23

6) PATRICK D. HOWARD. Guía para elaboración de políticas de seguridad. Internet: http:/www.unal.edu.co/seguridad/documentos/guia_para_elaborar_politicas_v1_0.pdf Acceso: 2010-04-10

7) UNIVERSIDAD DE LOS ANDES. Seguridad Informática. Internet: http://red.ula.ve/seguridad/politicas.php Acceso: 2010-02-26

8) ISO. Seminario ISO 27001. Internet. http://www.scribd.com/doc/24326153/Seminario-Iso-27001 Acceso: 2010-03-17

9) NIST. Computer Security Division – Special Publications (800 Series). Internet: http://csrc.nist.gov/publications/PubsSPs.html Acceso: 2010-02-17

10) IT Governance Institute. Cobit 4.0. Edición Español, IT Governance Institute, Estados Unidos, Junio del 2006. ISBN: 1-933284-37-4

11) LONG, Jhon O. ITIL® VERSION 3 AT A GLANCE. IBM. Springer. Estados Unidos – New York. 2008. ISBN: 978-0-387-77392-6

12) BLOG DE SEGURIDAD INFORMATICA. Análisis de Riesgos: ISO 27005 vs magerit y otras metodologías. Internet: http://seguinfo.wordpress.com/2009/10/30/analisis-de-riesgos-iso-27005-vs-magerit-y-otras-metodologias/ Acceso: 2010-04-05

13) SEGURINFO. Análisis y Gestión de Riesgos en TI ISO 27005 – Aplicación Práctica. Internet: http://www.segurinfo.org.ar/SITIO2009/Programa09/presentaciones/1610_ESET.pdf Acceso: 2010-04-29

14) IEPI. Instituto Ecuatoriano de Propiedad Intelectual – Ley de Transparencia/BaseLegal. Internet: http://www.iepi.gob.ec/files/LeyTransparencia/EstructuraOrganica/BaseLegal/Normas/RegistroOficial320LeyPropiedadIntelectual.pdf Acceso: 2011-02-17

15) SCOTT BESLEY, EUGENE F. GRIGHAM. Fundamentos de Administración Financiera. Décimosegunda Edición, McGRAW-HILL, México D.F., 2001. ISBN: 970-10-3084-2