UNIDAD ACADÉMICA:

DEPARTAMENTO DE INVESTIGACIÓN Y POSTGRADOS

TEMA:

DESARROLLO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LAS NORMAS INEN ISO/IEC27000 PARA EL MINISTERIO DE TRANSPORTE Y OBRAS PÚBLICAS.

Proyecto de Investigación y Desarrollo previo a la obtención del título de

Magíster en Gerencia Informática

Línea de Investigación, Innovación y Desarrollo principal:

Gerencia, Planificación, Organización, Dirección y/o Control de Empresas

Caracterización técnica del trabajo:

Desarrollo

Autora:

Verónica Elizabeth Defaz Toapanta

Director:

Darío Robayo Jácome Mg.

Ambato – Ecuador

Septiembre 2015

Desarrollo de un Plan De Seguridad de la Información basado en las Normas INEN ISO/IEC27000 para el Ministerio De Transporte y Obras Públicas

Informe de Trabajo de Titulación
presentado ante la
Pontificia Universidad Católica del
Ecuador Sede Ambato
por
Verónica Elizabeth Defaz Toapanta

En cumplimiento parcial
de los requisitos para el Grado
de Magíster en Gerencia
Informática

Departamento de Investigación y Postgrados
Septiembre 2015

Desarrollo de un Plan De Seguridad De La Información basado en las NORMAS INEN ISO/IEC27000 para el Ministerio De Transporte y Obras Públicas

Aprobado por:

Varna Hernández Junco, PhD
Presidente del Comité Calificador
Director DIP

Marcelo Balseca, Mg
Miembro Calificador

Dario Robayo Jacome, Mg
Director de Proyecto

Dr. Hugo Altamirano Villaroel
Secretario General

Dennis Chicaiza, Mg
Miembro Calificador

Fecha de aprobación:
Septiembre 2015

Ficha Técnica

Programa: Magíster en Gerencia Informática

Tema: Desarrollo de un plan de seguridad de la información basado en las Normas INEN ISO/IEC 27000 para el Ministerio de Transporte y Obras Públicas

Tipo de trabajo: Tesis

Clasificación técnica del trabajo: Desarrollo

Autor: Verónica Elizabeth Defaz Toapanta

Director: Darío Robayo Jácome, Mg.

Líneas de Investigación, Innovación y Desarrollo

Principal: Gerencia, Planificación, Organización, Dirección y/o

Control de Empresas.

Secundaria: Sistemas de Información y/o Nuevas Tecnologías de la Información y Comunicación y sus aplicaciones.

Resumen Ejecutivo

La entidades públicas hoy en día son entes principales de generación de información relevante de gran importancia, por lo que requieren de toda la seguridad para el cumplimiento de los procesos administrativos de los servicios que brindan a los usuarios y comunidad en general buscando eficiencia e integridad de la información, evitando que la misma sea tentación de pérdida, daños o modificaciones sin autorizaciones.

El desarrollo del presente proyecto es identificar las políticas de seguridad de la información basándose en las norma ISO 27000. Para el Ministerio de Transporte y Obras Públicas, para garantizar la confiabilidad, integridad y disponibilidad de la información que están contenidos en los activos de la institución como documentos, sistemas informáticos, medios de comunicación y otros.

La metodología implementada para el desarrollo del proyecto en mención es la metodología ISO, que es planificar, ejecutar, verificar y actuar, esta metodología es utilizada para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), para este proyecto solo se basa en la fase de planificación ya que para su implementación se debe contar con las autorizaciones de la máxima autoridad Srta. Ministra y contar con la partida presupuestaria necesaria de costo.

Declaración de Originalidad y Responsabilidad

Yo, Verónica Elizabeth Defaz Toapanta, portador de la cédula de ciudadanía y/o pasaporte No. 0502667298, declaro que los resultados obtenidos en el proyecto de titulación y presentados en el informe final, previo a la obtención del título de Magíster en Gerencia Tecnología, son absolutamente originales y personales. En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto, y luego de la redacción de este documento, son y serán de mi sola y exclusiva responsabilidad legal y académica.

Verónica Elizabeth Defaz Toapanta
0502667298

Una vez concluido una aurea labor en los estudios de la Maestría en Gerencia Informática, que al final se ve reflejada en el desarrollo del presente proyecto, el mismo quiero dedicarlo a Dios por sus bendiciones, a mi familia que han sido mi apoyo fundamental, a nuestro compañero y amigo Miguel Oviedo que lamentablemente en el transcurso de alcanzar este objetivo, nuestro señor lo llevo a su ceno y finalmente a mi mayor motivación quien me ha llenado de fuerzas y entusiasmo a seguir adelante con mis objetivos para mi pequeña princesa Paula Abigail.

Reconocimientos

Los conocimientos adquiridos durante la trayectoria de estudios de la Maestría, han sido de gran aporte para el desarrollo del presente proyecto, por lo cual quiero hacer un reconocimiento general a todos los docentes quienes impartieron sus enseñanzas durante el periodo que duró la misma.

La guía para el desarrollo del presente trabajo final de titulación de postgrados ha sido un apoyo fundamental el Mg. Darío Robayo Jácome, quien aportado con su conocimiento, tiempo y profesionalismo.

Resumen

Este proyecto pretende desarrollar un Plan de Seguridad de la Información basado en las normas INEN ISO/IEC 27000, para el Ministerio de Transporte y Obras Públicas (MTOP), con el fin de establecer políticas, normas y procedimientos de gestión en la administración de la seguridad de la información, minimizando las posibles amenazas ante las vulnerabilidades de la institución.

La metodología implementada en este proyecto es PDCA, de la ISO, conforme a la primera fase que es la planificación, que ha permitido estructurar el estudio para evaluar y analizar los activos de información de cada unidad administrativa.

La recopilación de información mediante entrevistas, encuestas, visitas en el sitio y la aplicación de la metodología en mención, se ha obtenido como resultado un análisis exhaustivo de los riesgos que se ven expuestos los activos, que para minimizar su impacto se los administrará de un tratamiento especial mediante la definición de políticas de seguridad, de acuerdo a los dominios y controles de la Norma ISO 27002.

Tomando en cuenta la importancia de los activos de la información para la institución, se sugiere realizar la implementación del proyecto dejando en consideración el cambio de las políticas definidas.

Abstract

This project aims to develop an Information Security Plan based on the INEN ISO / IEC 27000 standards for the Ministry of Transport and Public Works (MTOP), in order to establish policies, standards and procedures for managing the administration of information security, by reducing potential threats to the vulnerabilities of the institution.

The methodology implemented in this project is PDCA, ISO, according to the first phase which is the planning, that has allowed to structure the study to evaluate and analyze the information assets of each administrative unit. Information gathering through interviews, surveys, site visits and the implementation of the methodology in question was obtained as a result of a comprehensive analysis of the risks they are exposed , which in order to minimize its impact, special procedures will be managed by defining security policies, according to the domains and controls of ISO 27002.

Considering the importance of information assets to the institution, it is suggested to develop the project implementation taking into consideration the change of the defined policies.

Tabla de Contenidos

Lista de Tablas

Lista de Figuras

Capítulo 1

Introducción

La secretaria Nacional de Administración Pública ha emitido el Acuerdo 166, art 1 que dice ”Disponer a las entidades de la Administración Pública Central, Institucional, y que dependen de la Función Ejecutiva el uso obligatorio de las normas técnicas ecuatorianas INEN ISO/IEC 27000, para la gestión de la seguridad de la información”. Considerando este acuerdo y a su vez por las irregularidades que se han presentado en las entidades públicas en lo que se refiere al hurto de información lo cual han hecho hincapié una serie de perjuicios para la sociedad entera.

Esta situación ha surgido por el incumplimiento de controles, normas o políticas para la protección de la información. Se cita un ejemplo de fraude como el robo de 3,5 millones de dólares en el GAD Municipal Riobamba debido a un manejo indebido en la privacidad de las claves, entre otros.

El presente proyecto busca desarrollar un Plan de Seguridades de la Información, de una entidad pública de acuerdo a la realidad y bases para la implementación en otras entidades que deseen mejorar la gestión de las seguridades de la información dentro de sus respectivas necesidades organizacionales. Además, considerando que la Ley Orgánica de Entidades Públicas del Ecuador apoya el uso de sistemas informáticos basados en software no propietario, el producto de la documentación del Plan de Seguridades de la Información, teniendo apoyo de herramientas especializadas.

Para iniciar el proyecto se selecciona la entidad pública que servirá como Caso de Estudio, posteriormente se analizará el estado actual de la Seguridad de la Información en los departamentos que generen o manipulen información de gran importancia, considerando los Objetivos de Control de la norma NTE INEN-ISO/IEC 27000.

A partir de esto se procede a seleccionar los controles de los dominios de la norma NTE INEN-ISO/IEC 27001, 27002 a ser aplicados, considerando las necesidades más relevantes en el análisis, luego se definirá el Plan de Seguridades de la Información, que solvente las necesidades de seguridad identificadas.

Y por último se evaluará la aprobación e implementación del Plan dentro de las unidades de mayor vulnerabilidad de la información, cuando el proyecto Desarrollo del Plan de Seguridades de la Información, basado en las NORMAS NTE INEN-ISO/IEC 27000, estará a cargo de la entidad de estudio.

1.1. Presentación del trabajo

La necesidad de solventar las amenazas que hoy en día están atravesando las entidades públicas en la falta de seguridad de la información, se ve en la necesidad de buscar soluciones a los problemas, aplicando políticas de seguridad de la información.

La implementación de una metodología para el desarrollo de un Plan de Seguridades de la Información(PSI), ha permitido dar lineamientos de una aplicación sistemática para diseño, gestión y monitoreo [10], por lo que este proyecto tiene como alcance elaborar un Plan de Seguridad de la Información que no determine solo una metodología, sino que permita estructurar las políticas de gestión de acuerdo a las necesidades de la institución analizando e identificando que tipo de Normas Técnicas Ecuatorianas INEN-ISO/IEC 27000, centrándose en los procesos administrativos y el tipo de importancia de la información.

1.2. Descripción del documento

El presente documento abarca 6 capítulos distribuidos de la siguiente manera, Capítulo 1 Introducción, presentación del proyecto y descripción del documento, En el Capítulo 2 se plantea la propuesta de trabajo. El Marco Teórico es abordado en el Capítulo 3; en particular, la Sección 3.1 está dedicada a definiciones y conceptos, en tanto que la Sección 3.2 permite establecer el estado del arte. En el Capítulo 4 se presenta la Metodología; partiendo de la etapa de Diagnóstico (Sección 4.1), pasando por los Métodos particulares aplicados (Sección 4.2) para llegar a la descripción de Población y Muestra (Sección 4.4), la misma que no será aplicable a este proyecto. El Capítulo 5 está dedicado a la Presentación y Análisis de los Resultados del trabajo. Las Conclusiones y Recomendaciones son materia del Capítulo 6.

El trabajo está complementado por 5 Apéndices. El Apéndice A está reservado para Procedimientos Detallados. Por otro lado, algunos criterios adicionales para presentación del proyecto se enuncian en el Apéndice B, C, D.

Capítulo 2

Planteamiento de la Propuesta de Trabajo

Los avances en el desarrollo tecnológico han innovado a las entidades públicas implementar sistemas de tecnologías ya sean físicos, lógicos, etc., por lo cual muchos de los mismos se han visto inmersos a varias amenazas internas y externas como: personal no apto, programas maliciosos, hackers, siniestros, entre otros.

Las normas de seguridad tienen la finalidad de incluir dentro del plan lineamientos, medidas, métricas de los sistemas, identificación de riesgos y otros, pero en algunos casos no se ha obtenido resultados positivos por no implementar una buena metodología de un plan de seguridad de la información.

La Secretaría Nacional de Administración Pública ha emitido el Acuerdo 166, art 1 que dice "Disponer a las entidades de la Administración Pública Central, Institucional, y que dependen de la Función Ejecutiva el uso obligatorio de las normas técnicas ecuatorianas INEN ISO/IEC 27000, para la gestión de la seguridad de la información". Las áreas tecnológicas de las instituciones públicas han detectado varios riesgos de la información en la implementación de la tecnología; recalcando que la seguridad de la información no es similar a seguridad informática, sino también la parte física, personal y otros, el estar expuesto a la centralización de la materia tecnológica se embiste una estructura abstracta de la información, por tal motivo para mejorar la administración y crear políticas de seguridad se han visto inmersos en la implementación de nuevas técnicas que salvaguarden la integridad de la información, realizando un plan de seguridad de la información basándose en los estándares de norma INEN ISO/IEC 27000, ya que los mismos permiten adoptar un enfoque a la gestión de riesgos y mejorar los procesos, identificando métricas y medidas de protección.

El PSI propuesto, permitirá el control de la seguridad organizacional, lógica y física, que garantizará su confiabilidad, integridad y disponibilidad, creando políticas de seguridad (lógica, física, desarrollo y mantenimiento de sistemas informáticos), administración de las TIC, políticas de gestión periódica de activos, gestión de procesos operacionales y comunicaciones, administración de respaldo de información, gestión de auditoría y gestión de

amenaza y vulnerabilidades, aplicando la normativa de gestión de la seguridad de la información ISO/IEC 27000, minimizando los riesgos a los que se encuentran expuestos y alcanzando un alto control gerencial tecnológico implementando estrategias proactivas y reactivas a los cambios de los procesos operativos y sistemáticos, que las entidades públicas van atravesando; lo que se espera de la implantación de este plan es lograr un servicio de seguridad en el proceso de datos y transferencia de la información interna y externa, para contrarrestar los ataques maléficos de infiltración mediante la tecnología u otros medios, perfeccionando la gestión administrativa, alcanzando un alto grado de madurez en el manejo de la información y tecnología, para de esta manera cumplir con la metodología de implementación de SGSI(Sistema de Gestión de la Seguridad de la Información) y con el Acuerdo 166 art 1[9].

2.1. Información técnica básica

Tema: Desarrollo De Un Plan De Seguridad De La Información Basado En Las Normas INEN ISO/IEC27000 Para El Ministerio De Transporte Y Obras Públicas

Tipo de trabajo: Tesis

Clasificación técnica del trabajo: Tesis

Líneas de Investigación, Innovación y Desarrollo

Principal: Gerencia, Planificación, Organización, Dirección y/o Control de Empresas

Secundaria: Sistemas de Información y/o Nuevas Tecnologías de la Información y Comunicación y sus aplicaciones.

2.2. Descripción del problema

Las amenazas evolucionaron y también cambiaron algunos paradigmas de la seguridad. La frase «el enemigo está dentro» se popularizó hace ya unos años cuando los incidentes de seguridad cuyo origen estaba en el interior de las propias organizaciones comenzaron a aumentar. Dicho aumento cambió la percepción y el concepto de protección, puesto que hasta entonces las medidas de seguridad se centraban en crear barreras para proteger a las organizaciones de las amenazas externas [6]. Los avances en el desarrollo tecnológico han innovado a las entidades públicas implementar sistemas de tecnologías ya sean físicos, lógicos, etc., por lo cual muchos de los mismos se han visto inmersos a varias amenazas internas y externas como: personal no apto, programas maliciosos, hackers, siniestros, entre otros.

La seguridad de la información ya no puede ser concebida como el resultado de un accionar defensivo y reactivo para preservar los activos del negocio, ya que muchas veces, es un activo en sí mismo, una condición para operar y/o competir en el sector, un generador de valor. Requiere un accionar proactivo y su incorporación como elemento estratégico. [10] , las normas de seguridad tienen la finalidad de incluir dentro del plan lineamientos, medidas, métricas de los sistemas, identificación de riesgos y otros, pero en algunos casos no se ha obtenido resultados positivos por no implementar una buena metodología de un plan de seguridad de la información.

El desarrollo de un PSI es establecer las actividades y protocolos que deben ejecutarse para asegurar la confidencialidad, integridad y disponibilidades de los sistemas de información de la empresa. [3] y [1], por lo cual el presente proyecto permitirá promover seguridades de integridad, disponibilidad y confidencialidad de la información, implementando mejoras en las gestiones administrativas de la Información y la Comunicación, este plan permitirá identificar el/las áreas que más propensas estén expuestas a cualquier tipo de riesgos y poder tomar las decisiones de inmediato, verificando si es necesario ejecutar este plan en toda la institución o en dichas áreas más vulnerables que pueden ser la base de todos los procesos administrativos.

2.3. Preguntas básicas

¿Por qué se origina?

La falta de control en los incidentes de seguridad de la información amenaza la Confidencialidad, de garantizar la accesibilidad a la información exclusivamente a personal autorizado, desprotegiendo la integridad en los métodos de procesos, dando disponibilidad abierta a muchas amenazas de fuerzas mayor como: fallos de organización, humanos, técnicos provocando medios inseguros de protección.

¿Qué lo origina?

La implementación de nuevas tecnologías para la administración de la información, careciendo de un análisis de archivo sin adjudicaciones a la autorización de acceso, por negligencia o por ignorancia, cometiendo errores en la configuración de los parámetros y los programas, condicionando su seguridad.

2.4. Formulación de meta

Obtener un Plan de Seguridad de la Información, garantizando la adecuada aplicación de la política, normas y procedimientos de seguridad INEN ISO/IEC 27000.

2.5. Objetivos

2.5.1. Objetivo general.-

Desarrollar un Plan de Seguridad de la Información basado en las normas INEN ISO/IEC27000. (Ministerio de Transporte y Obras Públicas).

2.5.2. Objetivos específicos.-

1. Establecer políticas de gestión en la administración de la seguridad de la información
2. Realizar un análisis de las normas técnicas ecuatorianas INEN ISO/IEC 27000, de acuerdo a las políticas de gestión establecidas en el plan.
3. Diseñar las políticas, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información, de acuerdo a la metodología ISO que se aplicará en el proyecto.
4. Aplicar el Plan de Seguridad de Información al Ministerio de Transporte y Obras Públicas, una vez aprobado por la máxima Autoridad y disponibilidad de recursos.

2.6. Delimitación funcional

¿Qué será capaz de hacer el producto final del trabajo de titulación?

- Definir políticas, actividades, procesos, normas y protocolos que permitan realizar las tareas administrativas de manejo de la información con confiabilidad, integridad y disponibilidad.
- La Gestión de Activos permitirá aplicar una política de control de protección de un nivel alto de seguridad.
- Implementar políticas de gestión de personal o talento humano identificará los errores de responsabilidad del manejo de los medios de la información, evitando el manejo no adecuado de la misma.

- El implementar la Normas Técnicas Ecuatorianas ISO/IEC 27000, en el Plan de Seguridad de la Información, se logrará minimizar los riesgos y amenazas a las cuales se encuentra inmersa esta entidad pública.
- Otro proceso como la gestión física y ambiental, se debe determinar las políticas para evitar interrupciones en las actividades administrativos por eventos naturales, accidentes, fallas y otros.

¿Qué no será capaz de hacer el producto final del trabajo de titulación?

No aplica

Capítulo 3

Marco Teórico

3.1. Definiciones y conceptos

3.1.1 Evolución histórica de la seguridad de la información.

La evolución que se ha ido presentando en la última década habla de una situación compleja enfocándose en la tecnología como activo esencial para evitar amenazas mediante una gestión de riesgos, muchos expertos señalan que no existe el 100% de seguridad, por una comparación entre Seguridad Informática (medidas técnicas) y Seguridad de la Información (medidas organizativas).

La Seguridad de la Información es un concepto más global que persigue definir e integrar Políticas de Seguridad en los planes estratégicos, cuantificando los riesgos, se identifican aquellos más críticos para el negocio de forma continua, se plantean escenarios de crisis y se diseñan planes de continuidad de negocio y recuperación ante desastres, buscando una implicación de la gerencia y del personal directivo de la empresa, conozcan dónde y cómo utilizar las medidas técnicas de Seguridad Informática (línea operativa) en el marco de la Seguridad de la Información y sus medidas organizativas (línea estratégica).

Se puede decir que la seguridad de la información es la confidencialidad, integridad y disponibilidad de acceder a la información con gestión adecuada de los riesgos que se ven inmersos cotidianamente [18].

3.1.2 Seguridad informática.

Es salvaguardar la información mediante condiciones de sistema de procesamiento de datos y almacenamiento para protegerlos del impacto de daños de gran potencial en los sistemas informáticos o estructuras TIC.

3.1.3 Riesgos

La Normalización (ISO) define riesgo tecnológico como "La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole pérdidas o daños", considerando este concepto los riesgos son problemas que afectan a la vulnerabilidad de las actividades diarias de la institución o empresa.

3.1.4 Amenazas a la seguridad de la información.

Son incidentes reportados en el acceso a la información, entre estos se puede identificar las de tipo lógico, físico, humanas, desastres naturales y entre otros.

3.1.5 Normas ISO 27000

Es un conjunto de Estándares diseñados para proporcionar un marco de gestión de la seguridad de la información de cualquier organización pública o privada, las mismas que pueden ser implementadas en un Sistema de Gestión de Seguridad [7].

3.1.6 Normas ISO 27001

Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de2007), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados [7].

3.1.7 Normas ISO 27002

Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su

apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002 [7].

3.1.8 Normas ISO 27003

Consiste en una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el Anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación. [7].

3.1.9 Normas ISO 27005

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. 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 organización de la seguridad de la información. [7].

3.1.10 Modelo de Mejores Prácticas.

Se tiene varios modelos de mejores prácticas que permiten que permiten realizar planes estratégicos

Citamos algunos ejemplos:

ITIL (Information Technology Infrastructure Library), es un marco de trabajo de las buenas prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI). ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. [1].

(COBIT) “es un conjunto de mejores prácticas (marco) para tecnología de la información (TI) creado por la Auditoría de Sistemas de Información y Control Association (ISACA) y el IT Governance Institute (ITGI) en 1996. COBIT ofrece administradores, auditores y usuarios de TI

con un conjunto de aceptación general las medidas, indicadores, procesos y mejores prácticas para ayudarles a maximizar los beneficios procedentes de la utilización de tecnología de la información y el desarrollo adecuado gobierno de TI y de control en una empresa. [1].

ISO 271000 Contiene las mejores prácticas recomendadas en seguridad de la información para desarrollar, implementar y mantener especificaciones para los SGSI: ISO/IEC 27000- es un vocabulario estándar para el SGSI. [2].

3.1.11 Plan de Seguridad de la información.

Es un conjunto de políticas que se van definiendo de acuerdo a la identificación y evaluación de los riesgos ya sean de activos, tecnológicos y humanos, considerando las características administrativas de un negocio, organización e institución, planificando directrices indispensables para la gestión de la seguridad de la información.

3.1.12 Evaluación de los riesgos

Es un proceso de actividades que permite identificar vulnerabilidades, calcular o definir la escala de la base de los riesgos potenciales para diseñar e implementar las gestiones correspondientes para minimizar el impacto de los mismos.

3.1.13 Identificación de riesgos

Para proceder con este paso para identificar los factores que determinan el causal de los riesgos se puede utilizar **c**uestionarios de análisis de riesgos, Listas de chequeo de exposiciones a riesgo, listas de chequeo de políticas de seguridad, sistemas expertos generación de propósitos.

3.1.14 Análisis de riesgos

Es determinar la valoración de impacto y la ponderación de los factores para definir su prioridad de tratarlo.

3.1.15 Políticas de seguridad

Son lineamientos y procedimientos para adoptar estructuras elaboradas de manera personalizada recogiendo características propias de una organización, entidad o empresa

manteniendo la confiabilidad, integridad y disponibilidad de la información y recursos, tantos físicos, lógicos y humanos.

3.1.16 Sistema de Gestión de la Seguridad de la Información (SGSI).

Es el enfoque gerencial basado en la gestión de los riesgos de activos, recursos humanos, tecnológicos entre otros, para establecer políticas para una administración de la seguridad de la información con integridad, confiabilidad y disponibilidad.

3.2. Estado del Arte

El desarrollo de un Plan de Seguridad de la Información basado en las normas ISO/IEC, es la determinación de la información como un patrimonio muy importante, para garantizar la integridad, confiabilidad y disponibilidad de la misma.

El desarrollo de los Sistema de Seguridad de la Información, se orientan a la seguridad informática, infraestructura [2], la realización del PSI permitirá identificar los puntos más críticos en lo que se refiere a la parte física y sistemas, logrando regular el uso de estos servicios, mas no han logrado gestionar la seguridad de la información aplicando las normas de seguridad que hoy en día solicitan el cumplimiento las entidades certificadoras; las entidades públicas conforme al Acuerdo 166, dispone a la Administración Pública que dependen de la función Ejecutiva, el uso obligatorio de las normas técnicas ecuatorianas INEN ISO/IEC 27000 [9].

Se puede exponer que entidades públicas como CNT, ha implementado el Sistema de Gestión de Seguridad de la Información, logrando alcanzar el certificado de Seguridad de la Información, cabe recalcar que fue aplicado solo al proceso: "Venta e Instalación de Productos y Servicios de Datos e Internet para Clientes Corporativos", también se ha realizada un Sistema de Seguridad de la Información para la empresa ECUACOLOR, pero está más orientado a la seguridad informática.

La implementación de una metodología para el desarrollo de un PSI, ha permitido dar lineamientos de una aplicación sistemática para diseño, gestión y monitoreo [10], por lo que este proyecto tiene como alcance elaborar un Plan de Seguridad de la Información, que abarque todas la Unidades de la Matriz, Subsecretarías y Direcciones Provinciales del MTOP que determine varias metodologías de buenas prácticas, que permita estructurar las políticas de gestión de acuerdo a las necesidades de la institución analizando e identificando que tipo de Normas Técnicas Ecuatorianas INEN-ISO/IEC 27000, centrándose en los procesos

administrativos y el tipo de importancia de la información, para que dichas políticas de seguridad, corroboren la mitigación de los riesgos y se pueda implementar un solo SGSI a todos los procesos de la administración.

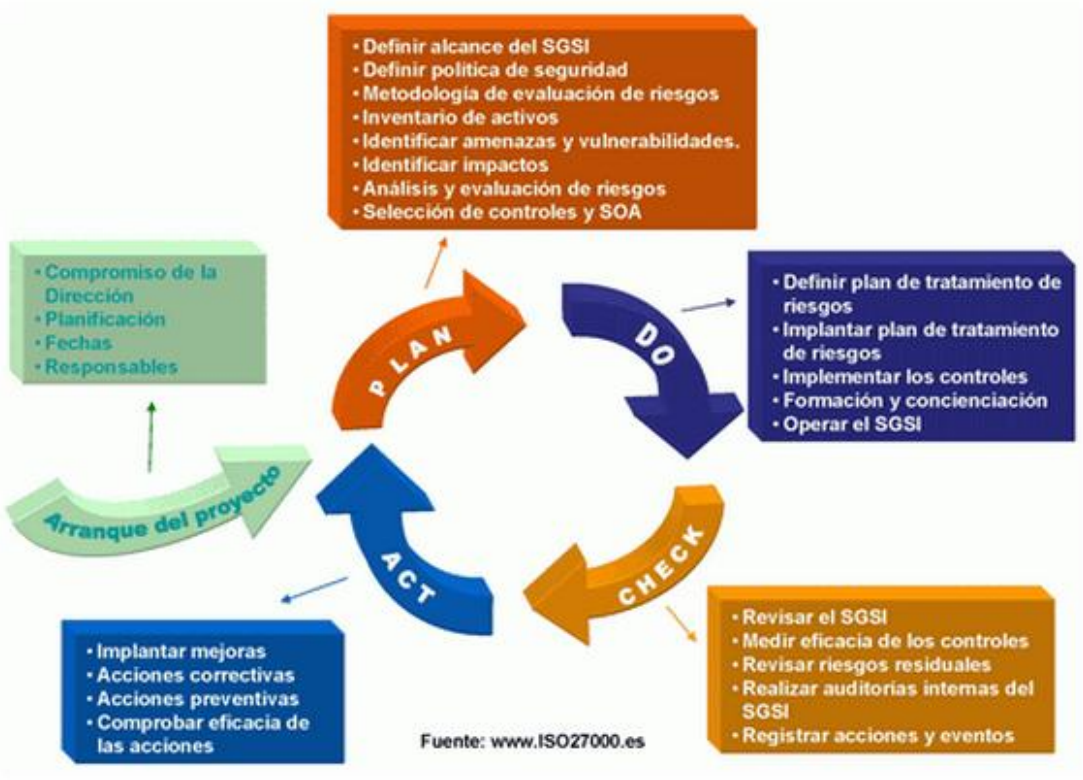
Capítulo 4

Metodología

Para el desarrollo del presente proyecto se utiliza la metodología PDAC (Planificar, Ejecutar, Verificar y Actuar), que establece las Normas ISO, en vista que es un Plan de Seguridad de la Información que se tomará en consideración para una entidad Pública como el Ministerio de Transporte y Obras Públicas, proceder con la parte de Planificación que comprende:

- Definir el alcance del plan de seguridad de la información, realizando entrevistas del estado actual de la seguridad de la información
- En base a la información obtenida analizar las políticas de seguridad.
- Analizar metodologías de evaluación de riesgos.
- Proceso de inventario de activos.
- Identificar amenazas y vulnerabilidades.
- Selección y Control de SOA
- Documentación final.

Figura 1: Metodología de Implementación SGSI**.**



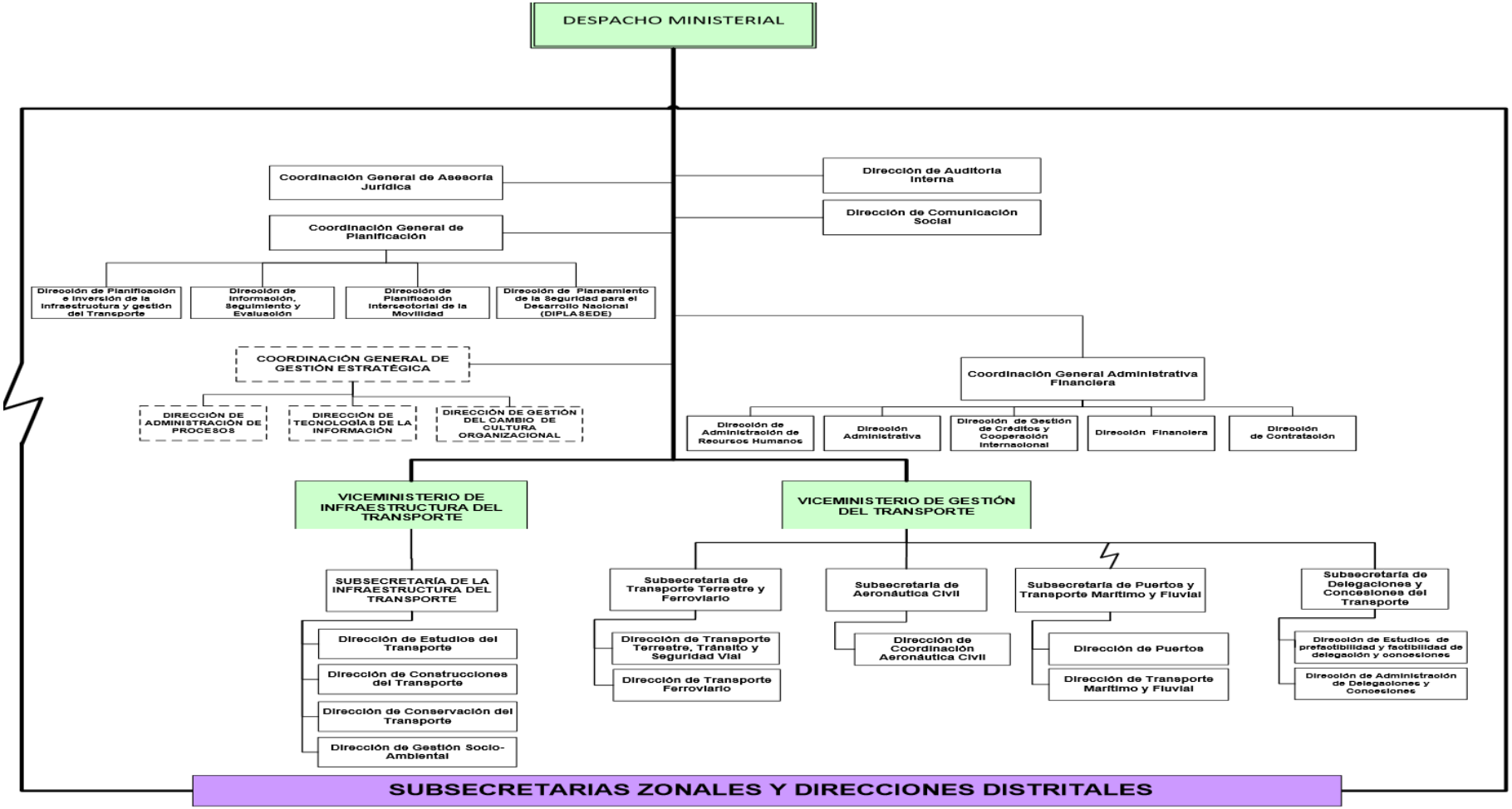
Fuente: http://www.iso27000.es/sgsi_implantar.html

4.1. Diagnóstico

Actualmente el Ministerio de Transporte y Obras Públicas, siendo un ente de gran importancia por la ejecución de proyectos de obras de miles de dólares, no han establecido políticas para salvaguardar la información, pero sobre todo obtener información íntegra, confiable y a la disponibilidad necesaria.

Para proceder con la recopilación de la información se ha realizado entrevistas no programadas en el sitio a los jefes y encuestas a los funcionarios de las unidades determinadas como: Tecnología, Planificación, Administración, Financiero, Recursos Humanos y Técnico conforme a un análisis de importancia de acuerdo al Organigrama Institucional.

Figura 2 : Organigrama Institucional MTOP



Fuente: http://www.obraspublicas.gob.ec/wp-content/uploads/downloads/2015/04/LOTAIP2015_literal_a1_organigrama_de_la_instituci%C3%B3n-1enero_2015.pdf

A parte de los mecanismos mencionados, el tener un muestreo entre las Direcciones Provinciales a nivel Nacional, para proceder con la recopilación de la información, en vista de los actos Administrativos, que han suscitado demora en los procesos, información errónea ingresada a los sistemas informáticos, perdida de documentación, personal no apto para realizar las actividades de supervisión, la no desactivación de servidores con cese de funciones, etc.

Con un recorrido y análisis en el sitio, se pudo determinar que la información más relevante se concentra en las Unidades de Financiero, Planificación, Técnico, Administrativo, Bodega, Archivo (General y Secretaria), Tecnología y Talento Humano, para constatar la seguridad de la misma, se procede aplicar 5 encuestas diferentes para cada Unidad, a excepción de la Unidad Tecnológica que se aplicaron 6 encuestas, obteniendo los siguientes resultados:

Tabla 1: Resultados De Entrevistas Realizadas.

UNIDAD	ENCUESTA 1	%	ENCUESTA 2	%	ENCUESTA 3	%	ENCUESTA 4	%
TECNOLOGIA	460	60,5	410	46,55	495	66	410	37,96
PLANIFICACION,FINANCIERO,AREA TECNICA	50	18,5	0	0	0	0	0	0
TALENTO HUMANO	102	72,9	0	0	0	0	0	0
ADMINISTRACIÓN, BODEGA	194	61,6	0	0	0	0	0	0
ARCHIVO	33	44	0	0	0	0	0	0

Fuente: Elaboración Propia.

En la tabla anterior se han realizado el cálculo de los resultados de las encuestas y se ha determinado un puntaje a las respuestas de toda la información requerida.

El trabajo de levantamiento de información está concluido, con esta información se procederá a identificar los riesgos de cada una de las unidades, ordenando y clasificando de acuerdo a prioridades.

4.2. Método aplicado.

El garantizar un nivel de protección total se podría manifestar que es algo imposible de realizar, por lo cual se espera obtener con el PSI una garantía de que los riesgos identificados se dé el tratamiento adecuado para que puedan ser solventados de manera documentada, con estructura eficiente y que sea adaptable a cambios conforme al entorno y las tecnologías.

Las Normas ISO permite definir los controles que se van a establecer en un PSI, por lo cual se analizan los 11 dominios y 133 controles de las ISO 27002[17].

4.2.1. Recopilación de Información de Seguridad

La recopilación de la información se ha procedido identificando las Unidades de trabajo del MTOP de mayor relevancia que manejen información de gran importancia, conforme a las observaciones en el sitio.

4.2.2 Políticas de Seguridad de la Información

Mediante el desarrollo del PSI, lo que se espera lograr es la protección de los recursos de información y tecnología del MTOP, que es utilizada para sus actividades diarias procesos administrativos, para cubrir las amenazas, ya sean internas, externas, deliberadas, accidentales, con el objetivo de asegurar que la información requerida demuestre la confidencialidad, integridad, disponibilidad, legalidad.

Al implementar las medidas de seguridad se identifica los recursos, partidas presupuestarias sin la necesidad de asignar partidas extras manteniendo las políticas de seguridad actualizada, manteniendo su vigencia y un alto nivel de eficiencia.

4.2.2.1 Aspectos Organizativos de la Seguridad de la Información

La administración de la Institución con los procesos de la seguridad de la información dentro de un marco administrativo debe permitir el control de la implementación del PSI determinando funciones y responsabilidades, fomentando la cooperación Institucional garantizando la aplicación de medidas de seguridad adecuadas.

4.2.2.2 Gestión de Activos

La Gestión de los activos garantizará que los activos de la información reciban un alto nivel de protección, permitiendo clasificar dicha información que señale su sensibilidad y criticidad, definiendo medidas de tratamiento especial, aplicando políticas a toda la administración de la información en el Ministerio, logrando identificar a los usuarios responsables de mantener actualizada la misma, definiendo funciones para obtener permisos de acceso a la información.

Actualmente en el MTOP, no existe una persona responsable de la seguridad de la documentación dejando como delegado a los Técnicos de Archivos, quienes manipulan la información sin identificar con exactitud el grado de importancia de la misma, cada usuario responsable entrega la documentación en físico sin follar las hojas, sin listado y peor aún sin archivos digitales de respaldo.

En lo que se refiere a equipos tecnológicos muchos de ellos se encuentran en estado obsoleto por daños ya sea por tiempo de funcionamiento o mal manejo, los mismos que no se han dado de baja, considerándose en bodega en funcionamiento, la maquinaria pesada no cuenta con un mantenimiento preventivo, el mismo lo realizan por emergencias viales o si se daña alguna parte de la misma, dificultando llevar un registro exacto de maquinarias a chatarrización y de igual forma con bienes que son ubicados en las unidades de bodega.

4.2.2.3 Seguridad Ligada a los Recursos Humanos

Conforme a la LOSEP a lo que se rigen los servidores públicos, todo contrato por servicios ocasionales debe ser de dos años, lo que a la instituciones públicas ocasionan dificultades en mantener la secuencias de los proyectos, en estos cambios brusco se ha podido observar que existe fuga de información, retraso en cumplimiento de actividades, incremento de rubros y a su vez proyectos dados por terminados unilateralmente por falta de seguimiento y por mala elaboración de la información antes de ser contratados.

Otra falencia que se ha podido identificar es la contratación de personal con poca experiencia y falta de ética profesional que asumen cargos de mucha responsabilidad, lo que implicado que se genere información errónea y mediante la misma la toma de decisiones equivocadas por parte de las Autoridades.

Finalmente muchos de los que han sido contratados no ejercen las funciones que se estipulan en el contrato, a su vez se rigen en las tareas que los jefes dispongan, de igual manera ocasionando daños severos en la documentación e información, por otro lado el momento de que los servidores salen de la institución no presentan informe de actividades pendientes y cumplidas, sin entregar la información correspondiente.

4.2.2.4 Seguridad Física y Ambiental

El edificio de la Administración Central del MTOP, en lo que se refiere a seguridad física las instalaciones cuentan con lo necesario pero no con lo indispensable para la seguridad en vista que se tiene accesos que no son monitoreados con la confianza de que por los mismos solo ingresan servidores de la institución.

En lo que se refiere a las instalaciones de las Direcciones no son aptas para mantener las seguridades necesarias para salvaguardar la información, ejemplos la Dirección Provincial de Tungurahua, la edificación es compartida con Correos del Ecuador y CNT, incluso con CNT se comparte puerta de ingreso, no existe puertas con seguridad eléctrica, para el ingreso a las oficinas existe puertas de vidrio con un cubre puerta de metal, son puertas muy sencillas de fácil manipulación, y las seguridades de las puertas del interior no existen, se puede ingresar por ventanas o abrirlas fácilmente.

Las especies físicas otorgadas para el almacenamiento de los archivos no cumplen con el reglamento general de conservación de archivos, no existe ventilación, iluminación, seguridades contra incendios, piso falso, estanterías, existen filtraciones de agua, y espacios reducidos.

En lo que se refiere a las seguridades ambientales las direcciones no cuentan con seguridades ambientales adecuadas, existe filtraciones de agua, humedad, no hay seguridades contra incendios, lo que sería muy susceptible a deterioro de los equipos tecnológicos incluyendo la documentación.

4.2.2.5 Gestión de Comunicaciones y Operaciones

La gestión de comunicaciones y operaciones nos permite generar políticas que aseguren la garantía del buen funcionamiento de la operación de los medios de instalación donde se procesa la información. La Unidad de Tecnología ha desarrollado el sistema SITOP (Sistema de Transporte y Obras Publicas), el mismo que está diseñado para administrar los proyectos en ejecución, administración de maquinaria pesada y vehículos, el cual se ha analizado y no cumple con las necesidades de los usuarios.

Por tal motivo con las nuevas políticas de seguridad debe incluir en el desarrollo los procedimientos de operación apropiados y la implementación adecuada para reducir el riesgo de negligencia o mal uso del sistema, documentando cada uno de los procedimientos requeridos o modificaciones realizadas, permitiendo tener información relevante para un proceso de auditoría y que se oriente a cambios.

4.2.2.6 Control de Acceso

Se hará referencia al control de acceso tanto a las edificaciones, documentación e información del MTOP, actualmente se ha podido constatar que no existen políticas de seguridad que permita controlar el acceso a los diferentes puntos, los usuarios ingresan sin una identificación, solo realizan un registro manual, no hay restricción al acceso de la información, se generan claves repetitivas, actualizan información de otros usuarios con usuario de administrador, todo esto se inclina a políticas definidas en la entidad pero sin un análisis previo para garantizar el acceso a la información de manera segura.

4.2.2.7 Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información.

Se busca gestionar la buena adquisición, desarrollo y mantenimiento de los sistemas de información como equipos de cómputo, software, maquinaria pesada y otros.

El adquirir estos recursos por el Portal de compras públicas ocasiona inconvenientes el momento de seleccionar el producto en vista que no cumplen con las características y se tiene que acoplar con la que más se asemeje o a su vez hay que realizar la adquisición con otros

proveedores, pero de igual manera se prefiere el de menos costo, dejando a un lado la calidad y beneficios.

Los sistemas informáticos que el MTOP, utiliza para cumplir con sus actividades, son administrados por otras entidades públicas, por lo que no se puede prescindir de un arreglo inmediato o definir los motivos de la caída de los sistemas, por tal motivo no se puede dar un mantenimiento preventivo a los mismos, mientras el SITOP sistema propio del MTOP, se encuentra con fallas en el diseño, no cumple con los requerimientos de los usuarios.

En lo que se refiere al mantenimiento de los equipos de tecnología, no se los realiza Mensualmente, solo cuando existen daños severos, lo cual ha provocado la pérdida de información

También se debe implementar una serie de políticas criptográficas con el objetivo de proteger los datos confidenciales de la institución, de personas que no están autorizadas a poseer dichos datos por cualquier motivo.

4.2.2.7 Gestión de Incidentes de la Seguridad de la Información

La gestión de eventos de seguridad de la información, los incidentes inesperados que tienen una probabilidad de amenazar los procesos administrativos, lo que al definir las políticas de seguridad permitirá disminuir la vulnerabilidad de la información asociada con los sistemas de información, logrando un aprendizaje de los mismos y buscando mecanismos para ser solventados para poder supervisar, el tipo de incidente, afectación y costos.

4.2.2.8 Gestión de la Continuidad de Procesos Administrativos del MTOP.

Las Políticas analizadas para ser implementadas, permiten que los procesos administrativos del MTOP, sigan su continuidad siendo capaz de solventar incidentes inesperados de alto o bajo nivel, permitiendo identificar los riesgos y determinar su tratamiento y mejorar los procesos y aumentar la rentabilidad de atención a los usuarios.

4.3 Aplicación de Metodología.

El considerar la metodología PDAC (Plan, Do, Check, Act) de la ISO para la elaboración de un SGSI, nos da a conocer que se debe cumplir 4 fases, planificar, ejecutar, verificar y actuar, en vista de ser una Entidad Pública la misma que para implementar cualquier proyecto primero se debe contar con la partida presupuestaria y autorización de la máxima Autoridad en este caso de la Srta. Ministra y que todos estos trámites gubernamentales consideran tiempo y una

planificación Anual, por tal motivo el desarrollo del proyecto en mención se basa en la fase de planificación para definir las políticas de seguridad y elaboración del PSI.

Se ha realizado un análisis exhaustivo a las Normas INEN ISO/IEC 27000, de las cuales a implementarse serian ISO 27001:2005/27002:2005, considerando las mismas por que han sido ya ejecutados en otros proyectos de empresas logrando alcanzar la certificación correspondiente y porque el MTOP está alcanzando el grado de madurez en la información, se espera la adaptación a este PSI, para luego migrar a las ISO 27001:2013/27002:2013, los mismos estándares han definido controles más aptos de entendimiento.

4.3.1 Planificar

En esta primera etapa se crean las condiciones para la realización del diseño, implementación y gestión del Sistema de Seguridad Tecnología, para lo cual se realiza un estudio de la situación del sistema informático desde el punto de vista de la seguridad, con el fin de determinar las acciones que se ejecutarán en función de las necesidades detectadas y con ello establecer las políticas, los objetivos, procesos y procedimientos de seguridad apropiados para dar un tratamiento exhaustivo a los riesgos y mejorar la seguridad de la información, con el objetivo de alcanzar excelentes resultados de acuerdo a las políticas y objetivos de la organización.

4.3.1.1. Alcance

El presente plan de seguridad de información pretende alcanzar una protección de todos los recursos que se denominan activos como hardware, software y documentos que contengan información, incluyendo personal de la organización, maximizando su ciclo de vida.

El mencionado plan servirá como un sustento a cualquier otra entidad y a su vez podrá ser implementado en todo el MTOP, considerando Subsecretarias y Direcciones Provinciales, para lo cual se deberá asignar responsables de las Unidades Administrativas, Tecnológica y Autoridades quienes serán los responsables de que dichas políticas de seguridad de la información sean cumplidas a cabalidad una vez se haya autorizado su implementación.

Este proyecto es muy amplio porque abarca niveles jerárquicos, los mismos que son encargados de la toma de decisiones condicionando la gestión de la seguridad de la información que debe implementarse a un SGSI.

La metodología aplicarse es una relación de integración vertical entre entidades públicas o empresas, en lo referente a los lineamientos de políticas en seguridad de la información.

4.3.1.2 Análisis de Metodologías de Evaluación de Riesgos.

Existe varios tipos de metodologías de evaluación de riesgos relacionados con la seguridad de la información como:

Metodología OCTAVE: Se basa en tres fases, visión de organización, tecnológica y planificación de medidas y reducción de riesgos, orientándose al aspecto técnico de la seguridad informática.

Metodología CORAS: Se basa en la elaboración de modelos utilizando lenguaje UML (Unified Modelling Language) y editor gráfico, y finalmente la Metodología de MAGERIT, que se basa en tres volúmenes métodos, elementos y técnicas.

Al realizar un análisis minucioso entre las metodologías descritas, para la evaluación y Gestión de Riesgos de los Sistemas de Información se utilizará la metodología de MAGERIT, "cumple con el objetivo primordial de garantizar la seguridad los sistemas de información, identificando problemas y definiendo políticas que los eviten. MAGERIT define los procedimientos que sirven de guía para el establecimiento de la protección necesaria de los sistemas de información de una institución de carácter público. Además, cumple con objetivos adicionales que están enfocados a la realización de un análisis de riesgos dentro de la institución. Estos objetivos son: Analizar los riesgos que soporta un determinado sistema de información y el entorno asociable con él, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio." [13].

Para realizar la gestión de los riesgos, considerando la aplicación de la metodología de MAGERIT, de acuerdo al primer volumen se detalla la identificación, evaluación y tratamiento de los riesgos, los mismos se obtendrán de las encuestas aplicadas a los servidores responsable [Apéndice B], en el segundo volumen se procede a determinar los activos de la institución que se obtendrán de la identificación de los riesgos y finalmente la técnica a utilizar es el análisis mediante tablas [Apéndices C y D].

Para la identificación de los riesgos se procedió a elaborar los bancos de preguntas con el propósito de recopilar información y determinar las falencias existentes en lo que se refiere a la seguridad de la información, las encuestas se establecieron a los servidores responsables de las unidades de RRHH, Tecnología, Administración, Planificación, Financiero, Técnicos, Secretaria, Archivo y Bodega, las mismas quedando de la siguiente manera [Apéndice A, encuestas].

Figura 3: Fases Gestión de Riesgos

Fuente: http://www.iso27000.es/download/doc_iso27000_all.pdf

Una vez que se ha recopilado la información se realizó una tabulación de los resultados teniendo los siguientes porcentajes.

Tabla 2: Porcentaje de resultados encuestas

UNIDADES ENCUESTADAS	PORCENTAJE DE RESULTADOS
TECNOLOGIA	43,67
PLANIFICACION,FINANCIERO, AREA TECNICA	18,5
TALENTO HUMANO	72,9
ADMINISTRACIÓN, BODEGA	61,6
SECRETARIA, ARCHIVO	44

Fuente: Elaboración Propia**.**

Los porcentajes se ha obtenido de las respuestas afirmativas, cada respuesta está valorada en un rango de 5 como máximo y 0 como mínimo, con estos resultados significa que hay un alto índice de inseguridad en la información, al tener los resultados de las encuestas se ha podido determinar los riesgos (Apéndice B), para la valoración de los incidentes se toma en cuenta del Articulo Técnico SGSI, de los autores Jaime Michilena y Paola Diaz (Apéndice C), adjunto Excel MATRIZ_RIESGOS_MTOP.

4.3.1.2.1 Determinación de Activos

Tabla 3: Determinación de Activos

Tipo de Activo	Activo
Servicios	Internet Correo Electrónico
Datos	Documentación Archivo Gestión interna
Aplicaciones	Software Quipux, GPR, SITOP, SIPeIP, ESIGEF Sistemas Operativos Sistema de Backup Antivirus
Bienes	Equipos de Red Maquinaria Pesada Bienes Muebles Bienes Inmuebles Seguridad Vigilancia
Redes de Comunicaciones	Telefonía IP Equipos de Acceso a Internet
Personal	Despacho Ministerial Coordinación General de Asesoría Jurídica Coordinación General de Planificación Dirección de Auditoria Interna Dirección de Comunicación Social Dirección de Planificación e Inversión Dirección de Información y Regula miento y Evaluación Dirección de la Movilidad Dirección de planeamiento de la seguridad del Desarrollo Nacional Dirección de Administración de procesos. Dirección de Tecnologías de la Información. Dirección de Cambio de Cultura Coordinación General Administrativa Financiera.

	Dirección Administrativa Dirección Financiera. Dirección de Talento Humano. Subsecretaria de Infraestructura de Transporte Dirección de Estudios Dirección de Construcciones Dirección de Conservación Subsecretarias Regionales Direcciones Provinciales.ie

Fuente: Elaboración Propia.

4.3.1.2.2 Ponderación de las Dimensiones de los Activos

Conforme a las encuestas realizadas se ha podido identificar los activos y considerar los daños que pueden ocasionar, para otorgar un valor y la importancia que tienen para la institución en cuanto a las dimensiones referenciadas como son Confiabilidad, Integridad y Disponibilidad, se dará un rango numérico en la escala de 5 a 1, de manera cualitativa (Apéndice D, Figura 5).

Tabla 4: Ponderación de Activos

ACTIVOS	DISPONIBILIDAD	CONFIABILIDAD	INTEGRIDAD	TOTAL
Internet	4	3	3	10
Correo Electrónico	5	3	3	11
Documentación Archivo	5	4	4	13
Gestión interna	4	3	3	10
Software Quipux, GPR, SITOP, SIPeIP, ESIGEF	4	3	3	10
Sistemas Operativos	5	4	4	13
Sistema de Backup	4	4	4	12
Antivirus	4	4	4	12
Equipos de Red	5	4	4	13

Maquinaria Pesada	4	4	4	12
Bienes Muebles	4	3	3	10
Bienes Inmuebles	4	4	4	12
Seguridad Vigilancia	5	3	3	11
Telefonía IP	5	4	4	13
Equipos de Acceso a Internet	5	3	3	11
Despacho Ministerial	3	3	3	9
Coordinación General de Asesoría Jurídica	4	4	4	12
Coordinación General de Planificación	5	4	4	13
Dirección de Auditoria Interna	4	4	4	12
Dirección de Comunicación Social	3	3	3	9
Dirección de Planificación e Inversión	4	4	4	12
Dirección de Información y Regulamiento y Evaluación	4	4	4	12
Dirección de la Movilidad	4	4	3	11
Dirección de planeamiento de la seguridad del Desarrollo Nacional	4	4	3	11
Dirección de Administración de procesos.	5	4	4	13
Dirección de Tecnologías de la Información.	5	4	4	13
Dirección de Cambio de Cultura	4	4	4	12

Coordinación General Administrativa Financiera.	5	4	4	13
Dirección Administrativa	4	4	4	12
Dirección Financiera.	4	4	4	12
Dirección de Talento Humano.	4	3	3	10
Subsecretaria de Infraestructura del Transporte	4	4	4	12
Dirección de Estudios	4	4	4	12
Dirección de Construcciones	4	4	4	12
Dirección de Conservación	4	4	4	12
Subsecretarias Regionales	4	4	4	12
Direcciones Provinciales.	4	4	4	12

Fuente: Elaboración Propia

4.3.1.2.3 Determinación de las Amenazas por Activo

Conforme a los activos se han determinado las amenazas que pueden incurrir en cada uno de ellos.

Tabla 5: Determinación de Amenazas de Activos.

ACTIVO	AMENAZAS
INTERNET	Uso inapropiado
	Acceso no autorizado
	Falta de servicio constante
	Interferencia
	Abuso de privilegios de acceso
	Manipulación de configuración de red
	Manipulación de programas
Correo Electrónico	Usurpación de identidad
	Falta de servicio
	Acceso no autorizado
	Bloqueo de correo
	Uso no previsto por otros usuarios
Documentación Archivo	Perdida de Información

	Deterioro de información
	Destrucción de la información
Gestión interna	Falta de energía eléctrica
	Manipulación de la configuración de los aplicativos
	Falta de planes estratégicos
	Falta de cultura tecnológica
	Divulgación de información
Software Quipux, GPR, SITOP, SIPeIP,ESIGEF	Ataque de virus
	Manipulación de programas
	Adquisición errónea
	Desactualización de la información
	Falta de requerimientos para desarrollo
	Errores de usuario
Sistemas Operativos	Suplantación de identidad de usuario
	Errores de administración
	Propagación de software malicioso
	Acceso no autorizado
Sistema de Backup	Manipulación de programas
	Suplantación de identidad de usuario
	Caída del servidor
	Falta de copias de seguridad base de datos
	Errores de usuario
Antivirus	Desactualización de antivirus
	Errores de administración
	Manipulación de programas
Equipos de Red	Acceso no autorizado
	Modificación de la asignación del equipo
	Accidentes imprevistos
	Falta de energía eléctrica
	Manipulación de las propiedades del equipo
	Ingreso no autorizado de equipo
	Manipulación de configuración de red
	Errores de administración
	Ausencia de puntos de red
Maquinaria Pesada	Desactualización de información
Bienes Muebles	Acceso no autorizado
	Accidentes imprevistos
	Falta de automatización inventario
	Cambio de ubicación de muebles no autorizado
Bienes Inmuebles	Desactualización de la información

	Edificaciones inseguras
	Inmuebles compartidos con otras instituciones
Seguridad Vigilancia	Falta de la credencial de acceso
	Usurpación de identidad
	Manipulación de registros mAnuales
	Robo o pérdida de equipos
Telefonía IP	Manipulación de asignación de IPs
	Falta de energía eléctrica
	Accidentes imprevistos
	Caída del servidor
Equipos de Acceso a Internet	Manipulación de configuración
	Accidentes imprevistos
	Caída del servidor proveedor
	Problemas con las conexiones del proveedor.
	Errores de administración
	Falta de energía eléctrica
servidores de las distintas unidades	Desconocimientos de sus funciones
	Asignación de actividades que no estipulan en el contrato
	Mala organización
	Indisponibilidad del personal
	Divulgación de información
	Extorsión
	Manipular información
	Destruir información

Fuente: Elaboración Propia

4.3.1.2.4 Calculo de Riesgos.

Los activos se han definido conforme al análisis de las amenazas que están englobados dentro de todos los procedimientos, de igual manera ha permitido identificar los riesgos que abarcan estos activos y a su vez cada proceso de gestión.

Tabla 6: Cálculo de Riesgos

ACTIVO	AMENAZAS	FRECUENCIA	IMPACTO	TOTAL
INTERNET	Uso inapropiado	3	4	7
	Acceso no autorizado	4	3	7
	Falta de servicio constante	2	2	4
	Interferencia	2	2	4
	Abuso de privilegios de acceso	4	4	8

	Manipulación de configuración de red	4	4	8
	Manipulación de programas	5	4	9
Correo Electrónico	Usurpación de identidad	3	4	7
	Falta de servicio	4	5	9
	Acceso no autorizado.	4	5	9
	Bloqueo de correo	4	4	8
	Uso no previsto por otros usuarios	4	3	7
Documentación Archivo	Perdida de Información	4	4	8
	Deterioro de información	3	4	7
	Destrucción de la información	3	4	7
Gestión interna	Falta de energía eléctrica	3	2	5
	Manipulación de la configuración de los aplicativos	4	4	8
	Falta de planes estratégicos	4	4	8
	Falta de cultura tecnológica	4	4	8
	Divulgación de información	4	4	8
Software Quipux, GPR, SITOP, SIPeIP,ESIGEF	Ataque de virus	4	4	8
	Manipulación de programas	4	4	8
	Adquisición errónea	3	4	7
	Desactualización de la información	4	5	9
	Falta de requerimientos para desarrollo	4	5	9
	Errores de usuario	3	4	7
Sistemas Operativos	Suplantación de identidad de usuario	3	4	7
	Errores de administración	4	3	7
	Propagación de software malicioso	4	4	8
	Acceso no autorizado	4	4	8
Sistema de Backup	Manipulación de programas	4	3	7
	Suplantación de identidad de usuario	4	4	8
	Caída del servidor	4	4	8

	Falta de copias de seguridad base de datos	4	4	8
Antivirus	Desactualización de antivirus	3	3	6
	Errores de administración	4	3	7
	Manipulación de programas	4	3	7
Equipos de Red	Acceso no autorizado	4	4	8
	Modificación de la asignación del equipo	4	4	8
	Accidentes imprevistos	3	3	6
	Falta de energía eléctrica	2	3	5
	Manipulación de las propiedades del equipo	4	4	8
	Ingreso no autorizado de equipo	4	4	8
	Manipulación de configuración de red	4	4	8
	Errores de administración	4	3	7
	Ausencia de puntos de red	4	4	8
Maquinaria Pesada	Desactualización de información	5	5	10
Bienes Muebles	Acceso no autorizado	4	4	8
	Accidentes imprevistos	4	3	7
	Falta de automatización inventario	4	3	7
	Cambio de ubicación de muebles no autorizado	4	3	7
Bienes Inmuebles	Desactualización de la información	4	3	7
	Edificaciones inseguras	4	4	8
	Inmuebles compartidos con otras instituciones	4	4	8
Seguridad Vigilancia	Falta de la credencial de acceso	4	4	8
	Usurpación de identidad	4	4	8
	manipulación de registros mAnuales	4	5	9
	Robo o pérdida de equipos	4	5	9
Telefonía IP	Manipulación de asignación de IPs	3	3	6
	Falta de energía eléctrica	2	3	5

	Accidentes imprevistos	3	3	6
	Caída del servidor	4	4	8
Equipos de Acceso a Internet	Manipulación de configuración	4	3	7
	Accidentes imprevistos	3	3	6
	Caída del servidor proveedor	4	4	8
	Problemas con las conexiones del proveedor	4	4	8
	Errores de administración	3	3	6
	Falta de energía eléctrica	2	2	4
servidores de las distintas unidades	Desconocimientos de sus funciones	4	4	8
	Asignación de actividades que no estipulan en el contrato	4	4	8
	Mala organización	4	3	7
	Indisponibilidad del personal	4	4	8
	Divulgación de información	4	4	8
	Extorsión	2	2	4
	Manipular información	4	4	8
	Destruir información	4	4	8

4.3.1.2.5 Plan de Tratamiento de Riesgo

Si tomamos en cuenta que los riesgos son las eventualidades de un objetivo y según la Organización Internacional por la Normalización (ISO) dice "La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole pérdidas o daños".

El tratamiento de los riesgos son las vulnerabilidades identificadas, así como las causas de los riesgos potenciales, los mismos han permitido cuantificar para que los responsables puedan tener información suficiente para realizar el diseño e implantación de los controles de políticas de seguridad y minimizar los riesgos existentes.

En vista de ser un tema demasiado extenso y mediante las encuestas realizadas se han procedido a identificar los riesgos considerando las amenazas identificadas, y a su vez se ha realizado un análisis, evaluación y tratamiento más exhaustivo. (Apéndice C).

Capítulo 5

Resultados

5.1 Determinación de resultados

Una vez analizada la situación actual de las seguridades del MTOP, se ha podido visualizar y constatar varias vulnerabilidades que han ocasionado serios problemas en los procesos administrativos, para lo cual las políticas a implementarse se basa en los controles ISO/IEC 27002[17], para custodiar los activos se debe establecer parámetros de procedimientos y controles de seguridad fundamentados en la evaluación de riesgos, que permitan gestionar eficientemente la accesibilidad a la información.

Dentro de los parámetros considerados como esenciales para el PSI se detalla los siguientes:

- Alinear los niveles de riesgo con el impacto organizacional.
- Mejorar la toma de decisiones.
- Analizar y ordenar la estructura de los sistemas de información.
- Definir procedimientos de trabajo para mantener su seguridad.
- Asegurar la confidencialidad, integridad y disponibilidad de la información.
- Optimizar las amenazas hasta alcanzar un nivel alto de seguridad por la institución.
- Continuidad de los procesos administrativos aun si se producen incidencias, minimizando el impacto y puedan ser controladas.
- Cumplir el marco legal de la legislación vigente.
- Alcanzar la certificación del Sistema de Gestión de Seguridad de la Información

Para conseguir la integración de los procesos administrativos, sistemas de información y los parámetros en mención se aplicará la norma ISO 27002, que contempla once dominios:

1. Política de Seguridad de la Información.
2. Organización de la Seguridad de la Información.
3. Gestión de Activos.
4. Seguridad de Recursos Humanos.

5. Seguridad Física y del Entorno.
6. Gestión de Comunicaciones y Operaciones.
7. Control de Acceso.
8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
9. Gestión de Incidentes de la Seguridad de la Información.
10. Gestión de la Continuidad del Negocio.
11. Cumplimiento.

5.1.1. Responsabilidades

La máxima Autoridad designará una Comisión para la Seguridad de la Información quienes sabrán asumir las siguientes responsabilidades.

- Presentar el Plan de Seguridad de la Información a las máximas Autoridades para su respectiva aprobación y continuar con las siguientes fases.
- Coordinar la ejecución, verificación y la actuación del PSI, para cumplir con el SGSI.
- Presentar informes del estado trimestralmente referente a la seguridad de la información al nivel autoridades, directores de unidades.
- Preparar auditorías que permitan verificar el cumplimiento del SGSI.
- Implementación de las políticas de la seguridad informática.
- Asesorías en materia legal referente a la seguridad de la información.
- Concientizar la seguridad de la información dentro de las responsabilidades.
- Establecer recursos financieros para mejorar las políticas de seguridad.
- Control exhaustivo de lo establecido en la política de seguridad de la Información por el personal a cargo.

5.1.2 Política de la Seguridad de la Información.

La Política de la seguridad de la información son las instrucciones globales que se ha definido para prevenir en un alto porcentaje los riesgos o incidentes en los procesos, considerando el cumplimiento de los objetivos de la institución tomando en cuenta las temáticas como el control de accesos, la clasificación de la información, la seguridad física y ambiental, uso de activos, escritorio y pantallas libres de información, etc., cumpliendo con los siguientes objetivos:

- Establecer Políticas de protección de los recursos de información del MTOP y los recursos tecnológicos utilizados para los procesos de las actividades diarias, asegurando la integridad, disponibilidad y confiabilidad de la información.
- Definir las políticas de seguridad para la elaboración del Plan de Seguridad de la información y garantizar el cumplimiento de los objetivos.
- Identificar los recursos y las partidas presupuestarias correspondientes, para proceder con la implementación de las políticas de seguridad.
- Definir periodos de actualización de las políticas de seguridad.
- Establecer sanciones por el incumplimiento de las Políticas de Seguridad de la Información.

5.1.2.1 Documento de la política de la información

Dentro de la documentación que se tiene que generar para una correcta aplicación son:

- Oficio de designación de Comisión de la Seguridad de la Información.
- Oficio de aprobación de las autoridades para la implementación del PSI.
- Registro de identificación de riesgos.
- Informe de conocimiento de riesgos.
- Informe de análisis y tratamiento de riesgos.
- Informe de nuevas políticas de seguridad aplicar.
- Informe de cumplimiento del SGSI.
- Informe de Resultados.

5.1.3. Aspectos Organizativos de la Seguridad De La Información

5. 1.3.1. Organización Interna

Autoridades se comprometen con la Seguridad de la información en los siguientes aspectos:

- Las Autoridades deben coordinar y autorizar las actividades de la Comisión designada para la Seguridad de la información.
- Designar recursos personales como económicos para la implementación del PSI.
- Cumplir con las políticas de seguridad y autorizar las respectivas sanciones del incumplimiento.

5. 1.3.2. Coordinación de la seguridad de la información.

La coordinación de las políticas de la seguridad de la información por quienes integran las Unidades del MTOP, identificando roles y funciones laborales.

La Unidad de Talento Humano es la responsable de socializar a los servidores públicos y trabajadores bajo el código de trabajo de la Matriz, Subsecretaria y Direcciones Provinciales, conozcan y apliquen las políticas de seguridad de la información.

De acuerdo a la designación de la comisión para Seguridad de la Información, se debe establecer una persona responsable de asumir las siguientes actividades:

- Identificar, analizar e implementar políticas que contemplan en el PSI y que serán definidos en el SGSI cuando sea implementado.
- Analizar los riesgos que al instante se pueden originar.
- Acorde a las políticas de la seguridad de la información detalladas en el PSI, asesorar al personal para la elaboración de los planes estratégicos institucionales de las Unidades pertinentes y la continuidad de los procesos en ejecución de proyectos.
- Analizar e implementar herramientas para cumplir con la seguridad de la información
- Actualizar de manera periódica (tres meses) los privilegios de acceso a los sistemas de información para fortalecer los controles de seguridad.
- Promover la cultura de aceptación frente a los cambios ante la implementación de seguridades de la información.
- Observar las nuevas amenazas y vulnerabilidades que pueden presentarse en los procesos y determinar los posibles tratamientos de seguridad.
- Realizar cronograma Anual de capacitaciones referentes a temas de seguridad de la información.
- Preparar pruebas de estudios de seguridad en todos los ambientes (Desarrollo, ejecución y Contingencia), para la autorización de la Comisión de Seguridad.

5.1.3.3. Asignación de responsabilidades relativas a la seguridad de la información.

La comisión asignada para la seguridad de la información se encarga de evaluar el PSI para control y verificación de los procesos de implementación a futuro del SGSI, bajo las siguientes responsabilidades:

- Revisar Anualmente estado general de la seguridad de la información.

- Monitorear los incidentes en la seguridad de la información, presentados en los procesos diarios.
- Aprobar posibles proyectos que salvaguarden la seguridad de la información.
- Actualizar nuevas políticas de seguridad de la información del PSI.
- Realizar un plan estratégico de identificación de amenazas.
- Elaborar informe de presupuesto necesario para la aplicación de nuevas políticas de seguridad.

Referente al personal asignado para informar y dar seguimiento del proceso del PSI y de la implementación del SGSI.

Tabla 7: Cuadro de Responsabilidades

CARGOS	FUNCIONES	RESPONSABILIDADES
Comisión de Seguridad de la información	Impulsar la implementación y cumplimiento de las políticas de seguridad determinadas en el PSI.	Informar del estado de la seguridad de la información a las autoridades esto se puede realizar cada 3 meses.
Dirección de Talento Humano	Socializar a los servidores públicos y personal a jornal de sus obligaciones respecto a su participación en los planes establecidos considerando el tratamiento de los riesgos.	Realizar seguimientos periódicos del cumplimiento a disposiciones referente al PSI e implementación del SGSI.
Coordinador Jurídico	Analizar la legalización de los contratos, acuerdos ministeriales u otra documentación realizada por los servidores o con terceros.	Asesorar legalmente al MTOP, conforme a las políticas de seguridad en el ambiente de su competencia.

Coordinador Financiero	Verificar, analizar y solicitar los recursos económicos para implementar y soportar las políticas de seguridad.	Informar trimestralmente los recursos financieros invertidos de acuerdo a las partidas presupuestarias asignadas a políticas de seguridad.
Director de Tecnologías	• Conocer, cumplir y socializar la Política de Seguridad vigente en lo que se refiere al ámbito tecnológico. • Cumplir con los requerimientos de seguridad de la información establecidos para la administración y operación de procesos que intervengan hardware, software y sistemas de información.	Determinación de los controles técnicos en seguridad información. Fiscalizar el cumplimiento de las políticas de seguridad en el ambiente tecnológico.
Director Administrativo	Verificar el cumplimiento de las políticas de seguridad.	Socializar a nivel Ministerial las Políticas de seguridad de la información en procesos, documentación recursos tecnológicos, humanos, bienes.

Fuente: Elaboración propia.

5.1.3.4. Proceso de Autorización de recursos para el proceso de la información.

La política definida para este punto al implementar se ha considerado la designación de una persona responsable de la información y del proceso, quien autoriza el tratamiento correspondiente, a su vez la comisión de la seguridad de la Información garantizara que el nuevo servicio cumple con las políticas de seguridad de la información definidas en este documento.

5.1.3.5. Acuerdos de confidencialidad

El MTOP posee acuerdos de no divulgación que reflejan las necesidades internas para la protección y seguridad de la información, los servidores, contratistas, proveedores y terceros que tengan contacto de actividades con el Ministerio, estos se han lógicos o físicos

involucrando manejo de información, se debe socializar y los mismos deben firmar aceptando la responsabilidad del acuerdo de confidencialidad de la información.

5.1.3.6. Revisión independiente de la seguridad de la información.

Las políticas de seguridad de la información que han sido definidos para los procedimientos, deben ser revisados para lo cual deberían realizar un cronograma independiente de otro tipo de sistemas por un organismo o consultor externo, siempre y cuando suceda cambios sustanciales en la información o a su vez Anualmente información de la organización, siguiendo los lineamientos ISO 27001.

5.1.3.7. Terceros.

5.1.3.7.1. Identificación de los riesgos derivados del acceso de usuarios

Conforme al acceso de información por terceros (usuarios u otras entidades) identificar los requerimientos de controles específicos:

- La comisión de seguridad en conjunto con el servidor propietario de la información documentar los accesos requeridos.
- Categorizar los tipos de acceso requerido ya sean de manera física o lógica.
- Solicitar documentos justificativos por el cual solicita la información.
- Determinar el valor cuantitativo de importancia de la información.

En los contratos en especial de servicios profesionales como vigilancia, mantenimiento de equipos de cómputo otros, se establecerán los controles de seguridad y la confidencialidad, antes de firmar los mismos.

5.1.3.7.2. Tratamiento de la seguridad en relación con los usuarios o terceros.

- Se realizara controles de seguridad de los activos de la Institución abarcando los activos físicos (hardware, documentos, dispositivos tecnológicos, otros), la información y el software.
- Establecer procedimientos para seguimiento de los eventos de pérdida o modificación de datos.
- Determinar controles con el objetivo de garantizar la recuperación o destrucción de la información dependiendo de la vigencia del contrato.
- Realizar restricciones de copia y divulgación de información.
- Determinar políticas de permiso de transferencia de personal a otras Instituciones.

- Políticas de Derechos de Propiedad Intelectual, registro de la propiedad intelectual en lo que se refiere a desarrollo de software.
- Establecer políticas de seguridad para la entrega de usuarios y contraseñas de los Sistemas de Información en vista de ser contratistas tienen que generar planillas y actualizar en los sistemas y manejo de documentación.
- Restricción de autorización de accesos y privilegios de usuarios.
- El Director de Tecnologías es la persona encargada de asignar a la persona responsable de la instalación y al mantenimiento de hardware y software, bajo el aval de la comisión de seguridad.
- Instalación de programas de detección de software malicioso.
- Informes diarios de incidentes relativos a la seguridad de la información.

5.1.4. Gestión de Activos

5.1.4.1. Inventarios de Activos

La política para el inventario de activos se establece la asociación con cada medio de información, en el mismo se determina el responsable y la ubicación del activo, una vez obtenida esta información se presenta el inventario general, el mismo que debe estar sujeto a cambios y actualizaciones en un período de tres meses, designando como responsable a cada Unidad de su elaboración.

5.1.4.2. Propiedad de los activos

El servidor responsable de la información es único autorizado que puede modificar el tipo de clasificación de la información, cumpliendo con los siguientes requisitos:

- Determinar tipo de clasificación.
- Registro de fecha de modificación de la clasificación.
- Realizar reportes de la nueva clasificación e informar a los propietarios de la misma.

La información clasificada ayuda a identificar los tratamientos necesarios para su seguridad ya sean los recursos administrativos, humanos y tecnológicos.

5.1.4.3. Clasificación de la información

Los activos para ser clasificados deben considera los aspectos principales de la seguridad de la información que son confiabilidad, integridad y disponibilidad, para lo cual se aplicaran las siguientes directrices.

5.1.4.3.1. Directrices de clasificación

La información del MTOP se encuentra en medios tecnológicos, documentación en físico, recursos humanos, por lo que de acuerdo a los aspectos principales se define las siguientes directrices:

Confiabilidad

- Clasificar la información sin restricciones permitida el acceso para todos.
- Clasificar la información con restricciones permitida el acceso solo a los servidores de la institución.
- Clasificación de la información confidencial solo autoridades.

Integridad

- Modificación de la información sin altera su contenido.
- La información modificada sin previa autorización ocasiona daños severos a la institución, sin tener la opción a recuperación.

Disponibilidad

- Acceso a la información sin restricciones no causaría daños a la institución.
- La información con restricciones y acceso no autorizado causa daños.
- De acuerdo a la importancia de la información se determina periodo de tiempos para que la misma sea inaccesible, este tiempo puede ser en meses, semanas y días.

Para la clasificación de la información se asignan valores en un rango de 0 a 5 definiendo las siguientes categorías:

Baja: de 0 no supera de 2

Media: supera de 2 no supera de 4

Alta: supera de 4 no supera de 5

5.1.4.4. Etiquetado y manipulado de la información

El etiquetado y manejo de la información se debe realizar de acuerdo a la clasificación, los mismos deben estar en formatos físicos y digitales, tomando en cuenta las políticas de rotulación de archivo como:

- Logotipo de la Institución.
- Numero de caja, carpeta, dispositivo, etc.
- Nombre de la Unidad responsable.
- Nombre del responsable de la información.
- Año de emisión de la información.
- Código.
- Detalle del contenido.
-

5.1.5. Seguridad Ligada a los de Recursos Humanos

5.1.5.1 Antes del empleo

5.1.5.1.1. Funciones y responsabilidades

La responsable de la Unidad de Talento Humanos se encarga de definir los perfiles de los puestos de los servidores públicos y personal a jornal, informando a todos el ingreso del nuevo personal y sus obligaciones ante las funciones referentes a la seguridad de la información realizando los compromisos de Confidencialidad y cumplimiento de las actividades de capacitación.

5.1.5.1.2. Investigación de antecedentes

Conforme a los riesgos analizados es una amenaza el no contar con referencias comprobadas del personal a contratar por tal motivo se debe cumplir con lo siguiente:

- Presentar por lo menos 3 cartas de recomendación con fecha estimada de contratación.
- Tener la referencia de los dos últimos trabajos con números de contacto de los jefes para la comunicación directa.
- Determinar las causas de cese de funciones en los trabajos anteriores.

5.1.5.1.3. Términos y condiciones de contratación

- Se debe cumplir con el reglamento de la LOSEP para los servidores públicos y código de trabajo para la contratación a jornal, considerando el reglamento interno del MTOP.
- Diseñar los perfiles de los puestos conforme a las necesidades de la institución.
- Especificar en el contrato las actividades a desempeñar y eliminar y demás actividades que disponga el jefe inmediato por políticas de seguridad.

5.1.5.2. Durante el empleo

5.1.5.2.1. Responsabilidades de la Dirección.

- Se encargara de evaluar las necesidades de la institución para definir los perfiles a contratar.
- Disponer a la comisión de la seguridad de la información y al responsable de Talento Humano cumplir con las políticas de contratación para salvaguardar la información.

5.1.5.2.2. Concienciación, formación y capacitación en seguridad de la información

Es obligación de las entidades públicas capacitar a su personal, para lo cual se debe incluir en el cronograma de capacitaciones, la capacitación referente a las políticas, normas y procedimientos de la seguridad de la información y la capacitación del uso correcto de las instalaciones y recursos de procesamiento de información.

5.1.5.2.3. Proceso disciplinario

El personal que sea contratado al inicio de sus funciones debe recibir material de oficina, la documentación pertinente de las actividades que va a realizar, usuarios, claves de acceso a los sistemas y control de personal, para lo cual debe firmar un documento de confiabilidad en el mismo que debe estar detallado las reglas o políticas de la seguridad de la información, una vez cumplido con la legalización el responsable de la Unidad Tecnológica asignara los permisos de acceso a los sistemas de información, de acuerdo a su perfil.

Por otra parte, se existiera modificaciones en las políticas de seguridad se actualizaría el documento de confiabilidad y se comunicara a todo el personal, a su vez de eventos suscitados ante la violación de las seguridades.

5.1.5.3 Cese de empleo o cambio de puesto de trabajo

5.1.5.3.1. Responsabilidad del cese o cambio

- El momento que el personal contratado o la institución decida presidir de sus funciones tendrá que presentar un informe detallando las actividades pendientes y concluidas anexando todo tipo de información que haya generado.
- El jefe inmediato emitirá un informe de aprobación y conformidad de cumplimiento del personal saliente.
- En la notificación de cese defunciones debe establecer la fecha exacta que el personal debe permanecer en la institución para que proceda con la entrega de información.

5.1.5.3.2. Devolución de activos

Con el aval del jefe inmediato, se procederá con la toma de los activos que estuvieron a cargo del personal saliente, para lo cual la comisión de la seguridad de la información constatara de la entrega de los mismos, esto se debe realizar el momento de la notificación de cese de funciones.

5.1.5.3.3. Retirada de los derechos de accesos

Conforme a la notificación los derechos de acceso serán retirados con el informe del jefe inmediato y la comisión de la seguridad de la información, determinando que no hay nada pendiente de recibir.

5.1.6. Seguridad Física y Ambiental

La gestión de la seguridad física y ambiental nos permite reducir las amenazas debido a daños ocasionados por accesos físicos no autorizados, definiendo las zonas restringidas y perímetros de seguridad; los factores ambientales permite la garantía del control de los equipos de procesamiento evitando interrupciones por eventos de causas físicas.

5.1.6.1.Áreas Seguras

5.1.6.1.1. Perímetros de seguridad física

En el MTOP los perímetros de seguridad se han definido con el objetivo de proteger los espacios asignados para el procesamiento de información y otros para evitar incidentes en el

funcionamiento adecuado de los activos, creando diversas medidas de control físicas, estableciendo los siguientes controles:

- Establecer y documentar el perímetro de seguridad.
- Las instalaciones de procesamiento de información deben estar dentro de un espacio de construcción sólida con puertas protegidas contra accesos no autorizados, sistemas de alarmas, cerraduras eléctricas.
- Restringir el acceso al centro de equipos de cómputo, ingreso exclusivamente al personal autorizado.
- Registro ingreso y salida considerando hora, fecha y motivos de ingreso.
- Establecer un plan estratégico para salvaguardar la información ante eventos naturales, incendios, humedad o hurto de información.
- Elaborar un reporte de los sitios protegidos detallando código de edificación, espacio de seguridad, activos a proteger y tipos protección física implementados.

5.1.6.1.2. Controles físicos de entrada

Para control de acceso físico la comisión de Seguridad de la información debe analizar el tipo de acceso, considerando lo siguiente:

- Controlar el ingreso y salida de los visitantes registrando la fecha, hora y motivo de ingreso.
- Controlar el acceso a la información clasificada y procesamiento de información, al personal de guardia se le debe facilitar de un listado de las personas autorizadas y tarjetas magnéticas.
- Implementar tarjetas magnetitas especiales para todo el personal encargado de los espacios protegidos.
- Revisar los registros de acceso a los espacios protegidos por auditoria interna, detallando fecha y hora.

5.1.6.1.3. Seguridad de oficinas, despacho e instalaciones

Conforme a la infraestructura de las edificaciones pertenecientes al MTOP para diseñar los espacios de protección se consideran las posibles eventualidades que se podrían presentar como social, desastres naturales u otros provocados por el hombre.

Se establecen las siguientes medidas de protección para áreas protegidas:

- En los edificios se defina señalización para la respectiva información preventiva, informativa y otras.
- Ubicar el equipamiento de trabajo como impresoras, fotocopiadoras, equipos de cómputo dentro de los espacios protegidos para evitar manipulación no autorizada.
- Los conserjes deben revisar las puertas y ventanas sean cerradas cuando se termine las horas laborables.
- Cambiar puertas de las instituciones colocar mayor seguridad.
- El personal de vigilancia establezca un control más minucioso ante el ingreso de visitantes.
- Elaborar un registro automatizado para el control del personal de vigilancia.
- Entrega de tarjeta magnética a los visitantes.

5.1.6.1.4 Seguridad de los equipos

5.1.6.1.4.1 Seguridad del cableado

El cableado de energía eléctrica y de comunicaciones se ha podido observar que se encuentran en condiciones aptas de funcionamiento pero a su vez se designa políticas de seguridad para la mejor conservación de los mismos.

- Cumplir con los requisitos técnicos de implementación de cableado estructurado incluyendo las IEEE.
- En vista de que las edificaciones han sido diseñadas y construidas en tiempos atrás, no se pudo determinar un diseño claro del cableado de red por lo que se puede mantener el mismo en canaletas de conducción o cual sea la necesidad implementar conductos blindados, cajas con cerraduras en los puntos terminales.
- En el plan estratégico de Tecnología incluir actualización de la red de cableado para una reestructuración para verificación y normas.

5.1.6.1.4.2 Mantenimiento de los equipos

- El mantenimiento de los equipos deberá estar considerado en el plan estratégico tecnológico donde se debe describir los tipos de equipo, responsable, tipo de mantenimiento, daños ocasionados, y el tipo de mantenimiento brindado.

- Determinar los equipos para tareas de mantenimiento preventivo, bajo la responsabilidad de la Unidad Tecnológica.
- Reporte de equipos en mantenimiento.
- Reporte de mantenimiento terminado de equipos.
- Restringir el servicio de mantenimiento solo personal autorizado.
- Registro de incidentes presentados y periodo.
- Realizar copias de resguardo de la información de los equipos.

5.1.6.1.4.2 Seguridad de los equipos fuera de las instalaciones

El uso de los equipos en el campo será bajo la responsabilidad de los servidores o trabajadores solicitantes, para lo cual se debe definir qué tipo de información generaran y su clasificación, para determinar la seguridad correspondiente.

5.1.6.1.4.3 Reutilización o retirada segura de equipos

Los equipos que deben ser dados de baja de los inventarios de los activos, considerando los daños ocasionados, equipos obsoletos, documentación, a su vez si los activos a retirar no guardan información importante se podrá dar por chatarrización o su vez se solicitara su destrucción total basándose en las leyes administrativas.

5.1.6.1.4.4 Retirada de materiales propia de la institución.

- Para la retirada de materiales de la institución ya sea equipos, información, hardware o software, se tendrá que tener el aval de las autoridades, comisión de la seguridad de la información y responsable de los activos en mención.
- Informe de justificativos de retiro de materiales de la institución.
- Presentar un informe trimestralmente de los activos retirados, los mismos que deben contar en los inventarios de activos.

5.1.7. Gestión de Comunicaciones y Operaciones

La Gestión de comunicaciones y operaciones busca el correcto funcionamiento de las instalaciones de procesamiento de la información y comunicaciones, estableciendo responsabilidades de la seguridad de la información los que determinan los requerimientos de

la seguridad y aprobando los servicios de mensajería para transportar la información de acuerdo a su clasificación**.**

5.1.7.1 Responsabilidades y procedimientos de operación

5.1.7.1.1. Documentación de los procedimientos de operación

La actualización de cada procedimiento operativo se debe documentar en los mismos se especifica las políticas y cambios realizados, siendo un respaldo para manejo de errores comunes y generales que pueden presentarse en la manipulación de la información.

5.1.7.1.2. Gestión de cambios

Para realizar los cambios en la gestión operacional y de comunicaciones se procede a definir procesos de control los mismos tienen que evaluarse por expertos para que cumplan las características técnicas y las seguridades respectivas para que puedan ser avaladas por la comisión de seguridad de la información, certificando que dichos cambios no alteren la información y se dé una correcta implementación.

Los mantenimientos que realiza la Secretaria Nacional de Administración en el Sistema a cargo QUPUX, en la aplicación de nuevos procedimientos que garantice la calidad y confiabilidad del servicios se debe coordinar e informar a los servidores públicos para que procedan aplicar otras políticas internas de seguridad y generación de la información, hasta que el proceso de reinicio se cumpla.

La comisión de seguridad de la información debe evaluar los procesos de instalación, cambio o mantenimiento de componentes dentro de los sistemas de información o comunicaciones.

5.1.7.1.3. Segregación de tareas

La segregación de tareas se busca reducir el riesgo en un incidente de mal uso accidental de los sistemas de información, para lo cual el control aplicar es la restricción del acceso a los activos, antes de aplicar este control se debería monitorear todas las modificaciones que realicen para que el comité de seguridad de la información tenga un esquema y verificar si el control es aceptable o no.

Mantener los medios de desarrollo, prueba y operación separada para minimizar los riesgos del acceso no autorizado, tomando en cuenta lo siguiente:

- Documentar los requerimientos del software en desarrollo para las pruebas y ejecución.
- Para el desarrollo de software establecer un servidor de pruebas.
- Definir perfiles para usuarios que están encargados del desarrollo para impedir su acceso directo a los sistemas operacionales.

5.1.7.2 Gestión de la provisión de servicio por terceros.

5.1.7.2.1. Provisión de servicios

- Implementar políticas de seguridad en los acuerdos ministeriales para el trabajo con terceras personas estableciendo cláusulas de cumplimiento en la seguridad de la información en los contratos.
- Entregar claves de acceso a los sistemas de información generando documentos de confidencialidad.
- La información ingresada por terceros la comisión de seguridad de la información, evaluara la integridad de la misma, para proceder con los trámites internos.
- Emitir informe de incidentes ocasionados por la información de terceros.
- Las autoridades deben estar informados de los acontecimientos suscitados por terceros para la toma de decisiones en los respectivos contratos.

5.1.7.2.2. Gestión de cambios en los servicios prestados por terceros.

Políticas de seguridad referente a la gestión de cambios que puedan ser realizados por terceros, se debería tomar en cuenta los siguientes controles:

- Documentar los requerimientos de cambios en el desarrollo de software.
- Cumplir con la contratación de servicios conforme a los acuerdos emitidos por SERCOP.
- Definir varios proveedores antes de seleccionarlos.
- Elaborar acuerdo de confidencialidad en la información que se le sea proporcionada para realizar los servicios.
- Los equipos no deben salir de las instalaciones para sus mantenimientos, los servicios de terceros deben realizar sus trabajos dentro de las entidades.

- La comisión elaborara un informe de verificación de los servidores públicos si no están en capacidades de realizar las actividades, antes de proceder con la contratación de terceros.

5.1.7.3. Planificación y aceptación del sistema

- La planificación y aceptación del sistema el objetivo es minimizar las fallas en el mismo, realizando una planificación anticipada para la verificación de la capacidad y disponibilidad de los recursos, incluyendo para proyectos futuros y reducir los riesgos.
- Documentar y comprobar los requerimientos en el desarrollo de los sistemas nuevos antes de su ejecución.

5.1.7.3.1. Gestión de capacidades.

- Establecer monitoreo de los recursos disponibles para proyecciones de los requerimientos de capacidad requerido para nuevos procesos del sistema.
- Elaborar controles para informar los problemas en la brevedad posible para la toma de decisiones.
- Determinar requerimientos a tendencias actuales verificando las capacidades para desarrollar nuevos sistemas que permitan automatizar procesos.
- Analizar costos de desarrollo de nuevos sistemas o implementar actualizaciones de sistemas existentes, y beneficios.
- La información generada debe proporcionarse a las autoridades proporcionando la seguridad en su integridad, confiabilidad y disponibilidad en el tiempo que ellos dispongan para evitar la dependencia del personal evitando una amenaza de fuga de la información.

5.1.7.3.2. Aceptación del sistema.

- Establecer políticas de cultura tecnológica para los servidores públicos para la aceptación a los cambios en los procesos de los sistemas de información nuevos.
- Realizar pruebas piloto en la implementación de actualizaciones o nuevas versiones que cumplan con los requerimientos del usuario.
- Los requerimientos para el desarrollo o actualizaciones deben estar documentados y aprobados por los responsables de cada proceso.
- La comisión de la seguridad define los procedimientos de los errores y planes de contingencia ante eventos.

- La aceptación de los cambios ayuda a obtener la certificación y acreditación verificando la implementación apropiadamente de los requerimientos de seguridad.

5.1.7.4. Protección Contra Código Maliciosos y Descargables.

La protección de la integridad del software nos permite tomar precauciones para la detección de códigos maliciosos como virus cómputo, virus de red y bombas lógicas.

5.1.7.4.1. Controles contra el código malicioso.

Para el control del código malicioso se debe considerar lo siguiente:

- No utilizar software que no estén aprobados por el comité de seguridad, Unidad de tecnología y autoridades.
- Realizar un cronograma de revisiones de software y la información de los sistemas, para identificar activos no autorizados.
- Implementar software detección de códigos maliciosos en computadoras y control preventivo incluyendo todos los archivos, medios electrónico y por la red.
- Determinar un servidor de correo electrónico para la revisión de los adjuntos y descargas de los correos electrónicos para evitar código malicioso.
- Determinar responsables para la identificación y protección de códigos maliciosos en los sistemas de información
- La protección ante los códigos maliciosos es prudente realizarlos durante el mantenimiento y procedimientos de emergencia.

5.1.7.5. Copias de seguridad

5.1.7.5.1. Copias de la seguridad de la información

La integridad y disponibilidad de la información se basa en los procedimientos e implementación de políticas de respaldo de información o backups para restauración oportuna, si fuese la necesidad.

- Realizar copias diarias de respaldo de la información y código de software, para minimizar el riesgo de pérdida de información por actualizaciones u otros eventos.
- Definir el nivel de respaldo de la información produciendo registros exactos de las copias de respaldo y documentar la restauración de la misma.

- Determinar medios de almacenamientos externos de la institución con la aprobación del comité de seguridad de la información.

5.1.7.6. Gestión de la seguridad de las redes

En este control se detalla las políticas para la protección de la información que se transitan en las redes y de la infraestructura de soporte, considerando un monitoreo del flujo de datos.

5.1.7.6.1. Controles de red

- Implementar controles para la seguridad de la información en las redes, y proteger los servicios de accesos no-autorizados, estableciendo responsabilidades y procedimientos de gestión salvaguardando la confidencialidad, integridad de los datos que transitan por las redes públicas
- Elaborar registros de ingreso y monitoreo de las acciones de seguridad relevantes.

5.1.7.6.2. Seguridad de servicios de red

En los contratos que se realiza con proveedores externos para la implementación de las redes, deben incluir una cláusula de seguridad de la información, características, niveles de servicio (provisión de conexiones, redes privadas, firewalls, detección de intrusos), derechos de auditoria, autenticación, codificación y conexión de red.

5.1.7.7. Manipulación de los soportes

Controlar y proteger físicamente los activos para evitar la divulgación, el acceso no autorizado, modificación, eliminación o destrucción de la información.

5.1.7.7.1. Gestión de los soportes extraíbles

- Realizar contratos con empresas que se encarguen de la destrucción de la información papeles y otros medios, incluir en el contrato una cláusula de seguridad de la información comprometiéndole a la no divulgación de la información a ser eliminada.
- Registrar la eliminación los activos ya no indispensables para la institución teniendo un respaldo para los procesos de auditoría.

- Retirada de soportes de información.
- Establecer procesos para manipular y etiquetar los activos conforme a clasificación
- Restricciones de acceso personal.
- Realizar copias de los activos antes de su eliminación.

5.1.7.7.2. Seguridad de la documentación del sistema

Determinar normas de seguridad de la documentación de los sistemas.

Registro de acceso a la documentación del sistema conforme a autorización de responsable y comité de seguridad.

5.1.7. 8. Intercambio de información.

- Este tipo de intercambio no realiza el MTOP, los sistemas que manejan se enlazan con otros sistemas solo con la información necesaria como consulta, por ejemplo el sistema documental QUIPUX se enlaza con información del registro civil.
- Implementar políticas de no divulgación de la información en los sistemas de Talento Humano que la misma es ingresada en sistemas proporcionados por el Ministerio de Trabajo.
- La información que se maneja en el Sistema Oficial de Compras Públicas debe estar a la disposición de todos.

5.1.7.8.1. Acuerdos de intercambio

- Designar personal responsable de control y notificaciones del ingreso de la información en sistemas que no son creados por el MTOP.
- Documentar los tipos de intercambio de información.

5.1.7.8.2. Soportes físicos en transito

- La documentación debe ir en sobres completamente sellados, con las etiquetas visibles y claras, para el remitente.
- Definir y aprobar las mensajerías autorizadas.

5.1.7.9. Servicios de comercio electrónico

La seguridad de los servicios de comercio electrónico es el uso seguro de la información, considerando la integridad y la disponibilidad de la información publicada electrónicamente.

5.1.7.9.1. Comercio electrónico

- De acuerdo a la clasificación de la información para entregar la misma a otra entidad pública, firmar el acuerdo de confiabilidad.
- Determinar los requerimientos para la confidencialidad, integridad, recepción de documentos de los contratos asociados con procesos de licitación y contratos, que se realizan mediante el Portal de Compras Públicas.
- Designación de servidor responsable de los procesos de publicación con resolución emitida por la máxima autoridad y aprobada por la comisión de seguridad.

5.1.7.9.2. Transacciones en línea

- La firma electrónica que utilizan las máximas autoridades se debe tramitar de manera personal y su manejo ser exclusivo sin acceso a ningún otro funcionario, es para la generación de documentos legalizados.
- Emitir certificaciones presupuestarias para los montos designados para los contratos de cualquier índole.
- Emitir documentos de autorización por la máxima autoridad de los procesos de pago.
- Adjuntar los documentos en mención en el sistema ESIGEF para proceder al pago.
- Generar clave a un segundo servidor que remplace al responsable de los pagos por diferentes razones.

5.1.7.9.2. Información puesta a disposición publica

- Conforme a la clasificación de la información determinar la disposición del público, con la aprobación de la comisión de la seguridad.
- Los artículos a publicarse por el área de comunicación tener la sumilla de aprobado por la máxima autoridad.

5.1.7.10. Supervisión

La supervisión permite detectar los eventos de procesos no autorizadas, para lo cual se debe monitorear los sistemas de información, utilizando las bitácoras de operador, registrando las fallas para la identificación de los problemas en los sistemas de información, controlando la efectividad de las políticas de acceso.

5.1.7.10.1 Registro de auditorias

- Realizar los reportes de auditoría de las actividades, excepciones e incidentes de seguridad de la información en un periodo de 3 meses para tener un monitoreo exhaustivo del control de acceso.
- Reporte de fechas, horas y detalles de incidentes importantes.
- Reporte de accesos fallidos.
- Reporte de archivos a los cuales accedieron sin autorización.
- Activar las seguridades de los sistemas de protección anti-virus y sistemas de detección.

5.1.7.10. 2. Supervisión del uso del sistema

- Informe de los resultados de las actividades de monitoreo.
- Reporte del nivel de monitoreo mediante una evaluación de los riesgos, detallando la información de accesos autorizados y no, operaciones, alertas y otros.

5.1.7.10.3. Registro de fallos.

- Realizar un reporte de las fallas reportadas por los servidores públicos, usuarios y sistemas de información.
- Seguimiento de los reportes de fallas para la emisión de un informe de solución de las mismas cumpliendo con las políticas de seguridad.
- Evaluar el impacto de las fallas y si son repetitivos y cuales ha sido el nivel de riesgos.

5.1.7.10.3. Sincronización de reloj

Sincronizar el reloj en tiempo real significa en hora estándar local, tomando en cuenta las especificaciones locales, esta sincronización ayudará a la exactitud de los registros de

auditoría, y control de ingreso y salida de personal, dicha información debe ser exacta para los trámites administrativos necesarios.

5.1.8. Control de Acceso

El control de acceso permite definir técnicas de identificación y autorización para la implementación de las políticas en el acceso a los sistemas de información, y activos de la institución.

5.1.8.1. Requisitos de negocio para el control de acceso

5.1.8.1.1 Política del control de acceso

- Determinar los requerimientos de seguridad de cada uno de los sistemas de información.
- Clasificar la información de los diferentes sistemas y redes.
- Elaborar reportes de procedimiento que permita autorizar los accesos necesarios por los usuarios a la información o sistemas
- La comisión de seguridad debe controlar actividades operativas de acceso las mismas deben ser documentadas.

5.1.8.1.2. Gestión de acceso de usuario

5.1.8.1.2.1. Registro de usuario

- Definir nombres de usuarios únicos que no permitan realizar acciones no autorizadas con el mismo.
- Realizar monitoreo del usuario para verificar la autorización asignada por el administrador, servidor, base de datos
- Elaborar un formulario para ser legalizado por el usuario en el mismo que especifique su autorización de acceso y privilegios.
- La Unidad de Tecnología no está autorizado en crear usuarios o dar privilegios sin previa autorización de la comisión de seguridad de la información.
- En el contrato de servicios del servidor público se establecerá una cláusula de sanciones por incumplimiento a la política de seguridad de la institución.

5.1.8.1.2.2. Gestión de privilegios

- Conforme a cada activo determinar los privilegios sistema operativo, sistema de administración de bases de datos.
- Establecer tiempo de vigencia de los privilegios asignados.
- Conforme a las autorizaciones los privilegios se asignaran a usuarios específicos para manejo de información relevante y a usuarios generales privilegios comunes para tareas básicas de operación del sistema.

5.1.8.1.2.3. Gestión de contraseñas de usuario

- Legalización de documento de no divulgación de contraseñas individual o grupal.
- Cambio de contraseñas iniciales que han sido asignadas la primera vez.
- Las contraseñas deben ser encriptadas.
- Para procesos de mayor seguridad como en la Unidad Financiera deben realizar la autenticación con otro tipo de tecnología biométrica verificación de huellas.

5.1.8.1.2.4. Revisión de los derechos de usuario

- Revisar los derechos de usuario para un control eficiente ante el acceso a la información.
- Determinar un control trimestral.
- Revisar los privilegios de las autorizaciones a los usuarios trimestralmente, para verificar que no se han otorgado privilegios sin autorización.

5.1.8.1.3. Responsabilidades de usuario

5.1.8.1.3.1 Uso de contraseña.

- Monitoreo de las contraseñas otorgadas a los servidores y terceros.
- Realizar un cambio periódico de tres meses las contraseñas o al presentarse eventos de indicio de acceso no permitido.
- La contraseña asignada deberá cumplir con las características emitidas por la comisión de seguridad.
- Al generar las contraseñas no utilizar antiguas.

5.1.8.1.4. Equipo de usuario desatendido

- Los servidores deben garantizar que los equipos desatendidos sean protegidos adecuadamente.
- Determinar protección específica para las estaciones de trabajo o servidores de archivos, contra accesos no autorizados.
- La comisión de la seguridad de la información en coordinación con la unidad de Talento Humano para socializar las tareas de concientización a todos los servidores y contratistas.
- Establecer protectores de pantalla con contraseña para evitar que otros servidores manipulen los sistemas abiertos en un computador.

5.1.8.2. Control de acceso a la red

5.1.8.2.1. Política de uso de los servicios de red

- Establecer reportes de conexiones inseguras de red que no poseen la seguridad correspondiente, para la implementación de políticas de seguridad la información.
- La comisión de seguridad de la información debe evaluar al responsable de la Unidad tecnológica a cargo de otorgar el acceso a los servicios y recursos de red, conforme a lo requerido por el Director de Tecnologías y a plan de seguridad de la información.
- Se determinara las conexiones importantes de la red que procesan información clasificada.
- Restringir el acceso a internet.

De acuerdo al resto de controles de red que establecen las ISO 27002 como son: autenticación de equipos en las redes, Diagnostico remoto y protección de los puertos de configuración, Segregación de las redes, Control de conexión de la red, Control de encaminamiento de la red, se debe proceder con la verificación de las políticas implementadas por el proveedor que han contratado para la instalación de las mismas, una vez presentado el respectivo informe la comisión de la seguridad de la información analizaran que controles son factibles implementar.

5.1.8.3. Control de acceso a los sistemas operativos

5.1.8.3.1. Procedimientos seguros de inicio de sesión

- Instalar un sistema operativo que sea compatible con las características de los equipos de cómputo.
- Generar un mensaje acceso autorizado solo al propietario del equipo de cómputo.
- Crear contraseña única para el ingreso a los sistemas.
- Realizar reportes de intentos fallidos por ingreso no autorizado.

5.1.8.3.2 Identificación y autentificación de usuario

- Determinar un ID que identifique al usuario de manejo del sistemas operativos.
- Utilizar herramientas generadores de autentificaciones.
- Eliminar la autentificación de servidores cuando cesen sus funciones.

5.1.8.3.3 Sistema de gestión de contraseña

- Disponer el uso de contraseñas individuales para determinar responsabilidades.
- Crear contraseñas con la opción que los servidores cambien las mismas.
- Reporte de contraseñas utilizadas y no reutilizarlas.
- Poseer un archivo individual de la información de contraseñas y sistemas de aplicación.
- Realizar encriptado de contraseñas.

5.1.9 Adquisición, Desarrollo y Mantenimiento De Los Sistemas De Información

5.1.9.1. Requisitos de seguridad de los sistemas de información

5.1.9.1.1. Análisis y especificaciones de los requisitos de seguridad

- Especificación de requerimientos de seguridad para el desarrollo de aplicaciones o proyectos.
- Documentar el proceso de desarrollo de aplicaciones.
- Requerimientos de validación de información de ingreso a los sistemas.
- Generar reporte de controles automatizados y manuales que serán incorporados en los sistemas de información.

- Los requerimientos de seguridad deben determinar el valor del activo de información y el daño ocasionado por los incidentes.
- Los activos adquiridos como software u otros proceder con las pruebas previo a la aceptación de la comisión de la seguridad de la información.

5.1.10. Gestión De Incidentes De La Seguridad De La Información

5.1.10.1. Notificación de eventos y puntos débiles de la seguridad de la información

5.1.10.1. 1. Notificación de los eventos de la seguridad de la información

Los propietarios de la información deben notificar de los incidentes presentados en el día, especificando fecha, hora y tipo de incidente.

5.1.10.1. 2. Notificación de los puntos débiles de la seguridad

- Con las notificaciones presentadas por los propietarios de la información de los incidentes, el responsable del control de la información y la comisión de la seguridad de la información debe determinar los puntos débiles en los cuales se generó los incidentes.
- Generar reporte de incidentes.

5.1.10.1. 3. Recopilación de evidencia

- De acuerdo a los resultados de auditoría definir si los controles implementados de seguridad son los correctos y el archivo log no se ha modificado hasta su respectivo análisis.
- Informe de copias de respaldo de la información requerida.
- Reportes de resultado de auditoria.

5.1.11. Gestión de la Continuidad

5.1.11.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio

5.1.11.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio

- Desarrollar políticas de continuidad de negocio.

- Priorizar los riesgos identificando los más vulnerables hasta los de menor prioridad.
- Interpretar el impacto de las interrupciones en las actividades ocasionadas por incidentes.
- Asegurar la integridad del talento humano y de los activos de información.
- Documentar los planes de contingencia para prevenir interrupciones de servicio.

5.1.11.1.2. Continuidad del negocio y evaluación de los riesgos

- La continuidad es la relación con la identificación de incidentes que causan interrupciones en los procesos del MTOP, fallas de tipo eléctrico, errores humanos, desastres naturales, incendios y otros
- Los incidentes deben ser evaluados eventos en caso de ocurrencia, y que el servicio no se vea afectado.
- La evaluación de los riesgos implicados en la continuidad de las operaciones se debe contar con el apoyo de los propietarios de la información.

5.1.11.1.3. Desarrollo e implementación de planes de continuidad que incluya seguridad de la información.

Según los niveles establecidos implementar los procedimientos de recuperación y restauración de las operaciones.

Documentar detalladamente todos los procesos y controles aplicados.

5.1.11.1.4. Marco de referencia para la planificación de la contabilidad del negocio.

- Elaborar procedimientos temporales de orden técnico que aseguran una recuperación y restauración exitosa de los servicios.
- Determinar proceso de reanudación de los sistemas de información.
- Elaborar matriz de responsabilidad de los servidores implicados.

5.1.11.1.5. Pruebas mantenimiento y reevaluación de planes de continuidad.

- Elaborar un plan de pruebas de evaluación de la continuidad de las operaciones.
- Realizar pruebas flexibles de simulación utilizando diferentes escenarios y periodos de incidentes.
- Elaborar pruebas técnicas de operación, para la recuperación de información.

5.1.12. Cumplimiento

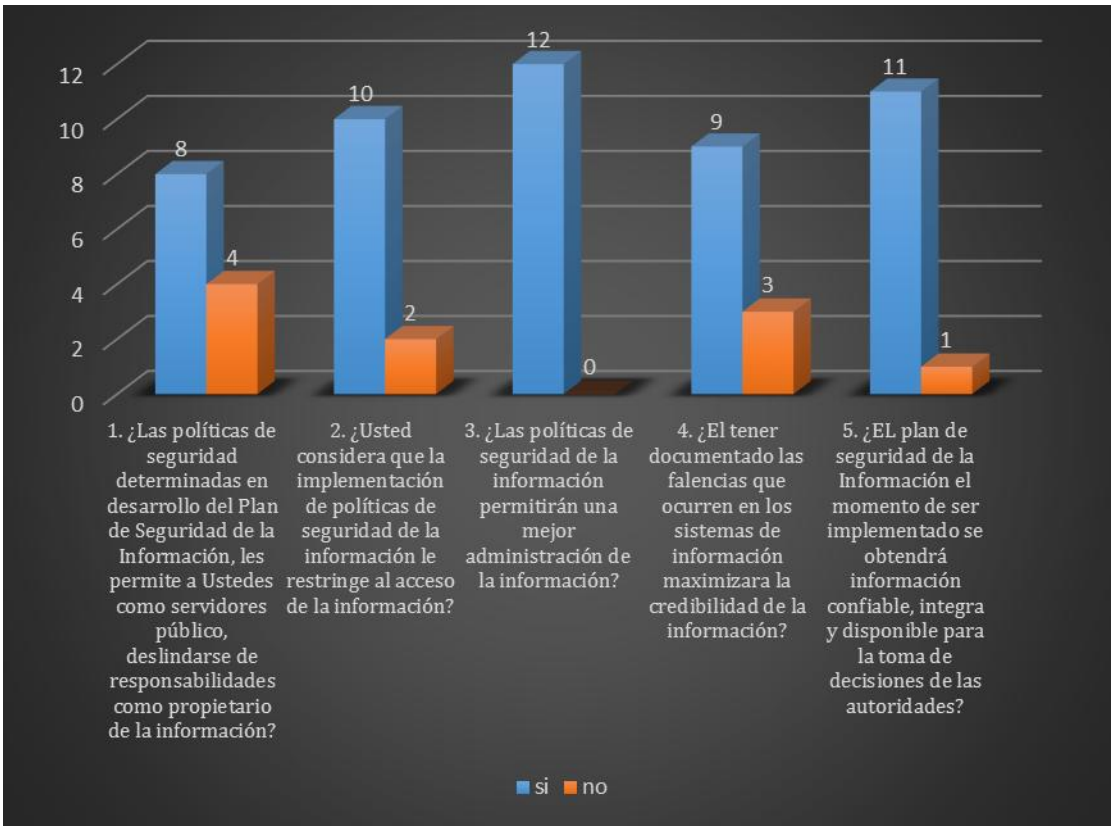
5.1.12.1. Cumplimiento de las políticas y normas de seguridad y cumplimento técnico.

- Conforme al resultado de revisión permitirá determinar los motivos de incumplimiento.
- Definir las acciones para eliminar el incumplimiento.
- La política de seguridad en los sistemas permitan realizar análisis exhaustivos sobre los mismos, estos análisis deberán ser realizados por un experto por la comisión de la seguridad de la información.
- Realizar las pruebas de vulnerabilidad de manera controlada y planificada con la respectiva documentación.

5.2. Evaluación Preliminar

El desarrollo de este Plan de Seguridad de la Información ha permitido introducirse en el ámbito administrativo del Ministerio de Transporte y Obras Publicas evidenciado los problemas que se suscitan en la seguridad de la información, se ha procedido a realizar unas encuestas a un representante de las unidades de Planificación, Financiero, Tecnología, Administrativo, Bodega, Archivo, Secretaria y Técnica de como actuaría ante la implementación de políticas de seguridad de la información formulando 5 preguntas básicas. (Apéndice D).

Figura 4: Resultados de encuestas



Fuente: Elaboración propia

Se ha procedido a evaluar los posibles cambios que se obtendrá con la implementación de un Plan de Seguridad de la Información en el MTOP a 12 servidores de las Unidades Principales, interpretando lo siguiente:

- Conforme a la pregunta N1, referente a deslindarse de responsabilidades de la información, 8 de 12 respondieron que si,lo que significa que la mayoría evaden las responsabilidades en la seguridad de la información, por tal motivo el implementar las políticas se aplicaría responsabilidades.
- Referente a la pregunta N2. De restricciones a la información, 10 encuestados manifestaron que si, lo que significa que al implementar las políticas de seguridad de la información se procede a la restrinción de la misma con el objetivo de salvaguardarla.
- Pregunta N3, referente ala administración de la información, de los 12 encuestados, todos respondieron que si, dando como resultado que la implementación de las políticas de seguridad mejorará los procesos administrativos, por consiguiente se mejora la seguridad de la información.

- En loque se refiere a la pregunta N4, la respuesta positiva de los 9 encuestados, a la documentación de las falencias presentadas, significa que la documentación a tratar de los incidentes permitiría tener un mejor control en la seguridad.
- Y Finalmente en la pregunta N5, los 11 encuestados dieron una respuesta positiva, referente a la correcta toma de decisiones de las autoridades, lo que hace referencia que la información con credibilidad permite mejorar la administración.

Como se puede observar en los resultados el Plan de Seguridad de la Información es aceptable para su implmentacion.

5.3. Análisis de resultados

El presente proyecto se ha podido constatar en los resultados de las políticas de seguridad definidas de acuerdo a los controles de la ISO 27002, son políticas que se encajan a los procedimientos de las actividades administrativas las mismas que han ido generando incidentes por el mal manejo de la información y de los activos que cuenta la institución, si se detalla un ejemplo en el cual se tiene uno de los riesgos identificados en la parte administrativa es el registro de ingreso y salida de los visitantes, por no tener las seguridades necesarias en las instalaciones físicas y tarjetas magnéticas o el guardia no se encuentra en su lugar de trabajo, han ingresado personas sin registro por lo cual ha causado perdida de información por el robo de computadores de los técnicos que se encuentran al frente de proyectos de gran importancia.

De acuerdo a este riesgo el control que se ha aplicado es el Dominio SEGURIDAD FÍSICA, el control de seguridad física de entradas, planteando la política de colocar puertas eléctricas que solo permita el ingreso al pasar la tarjeta magnética del visitante, de esta manera se está cumpliendo con los objetivos de establecer políticas de seguridad, analizar los controles de las normas técnicas ecuatorianas INEN ISO/IEC 27000.

De acuerdo a otros trabajos realizados en los que identifican los puntos más críticos en lo que se refiere a la parte de infraestructura y sistemas, logrando regular el uso de estos servicios, mas no han logrado gestionar la seguridad de la información aplicando las normas de seguridad que hoy en día solicitan el cumplimiento las entidades certificadoras; las entidades públicas conforme al Acuerdo 166, dispone a la Administración Pública.

Capítulo 6

Conclusiones y Recomendaciones

6.1. Conclusiones

- Se constató que en el Ministerio de Transporte y Obras Públicas se tienen controles de seguridad implementados pero que no han sido formalmente documentados, y a su vez no se han dado a conocer al resto como Subsecretaría y Direcciones Provinciales, motivo por el cual no se tomaron en cuenta para el desarrollo de este plan para el análisis de las norma NTE INEN-ISO/IEC 27001.
- El tratamiento de los riesgos adoptó una política de aceptación de los activos de información, recayendo en el más crítico, los Sistemas de información, para aplicar los controles de la norma NTE INEN-ISO/IEC 27002 y mejorar el estado actual de la seguridad de la información.
- Las políticas de seguridad detalladas en el Plan de Seguridad de la Información son los controles de seguridad que determinan el tratamiento del riesgo, dicho plan está a disposición de modificaciones para incluir nuevos controles antes de su respectiva aprobación de implementación.

6.2. Recomendaciones

- La implementación de los controles de seguridad en una institución deben estar legalmente documentados para sustento de la evaluación del estado actual de la seguridad de la información, de tal manera se socializa al personal mediante resoluciones, políticas, etc., garantizando la protección de los activos de información teniendo constancia de los controles implementados.

- La implementación del plan de Seguridad de la Información, debe ser realizado por un experto en la materia NORMAS ISO 27000, quien podrá avalizar si los controles detallados en el plan son los correctos para ser implementados, en vista de ser un proyecto de tesis no se tiene la aceptación de todos los servidores públicos para colaborar con la información necesaria para el desarrollo del presente proyecto.

Apéndice A

Encuestas

Encuesta Unidad de Archivo

1. **¿**Existe Políticas de Seguridad de la Información?
2. ¿Existe un Plan Estratégico para el control de los Archivos?
3. ¿Qué tipo de sistema utiliza para automatizar la información?
4. ¿Cuentan con un Sistema de Control de Archivos?
5. ¿Existen Normas para la conservación de los documentos de Archivo?

Encuesta Área Administrativa y Bodega.

1. ¿Existe un Plan de Vigilancia implementado en el MTOP?
2. ¿Existe alguna autorización permanente de estancia de personal ajeno a la institución?
3. ¿Quiénes saben cuáles son las personas autorizadas de ingresar al MTOP?
4. Además de la tarjeta magnética de identificación, ¿hay otras especiales para los visitantes?
5. ¿Se pregunta a los visitantes a que Unidad y a quien van visitar?
6. ¿Cómo se controla el horario de visitas?
7. ¿Existe Controles Automáticos para el Ingreso al MTOP?
8. ¿Quedan registradas todas las entradas y salidas al MTOP?
9. Al final de cada turno, ¿Se controla el número de entradas y salidas del personal y visitas de la Institución?
10. ¿Puede salirse del MTOP sin registro alguno
11. ¿Existe vigilantes las 24 horas?
12. ¿Existen cámaras de vigilancia?
13. Identificadas las visitas, ¿Se les acompaña hasta la persona que desean ver?
14. ¿Qué tipo de control especial aplican en la vigilancia por la noche?
15. ¿Existe una adecuada política de registros del personal y visitantes?
16. ¿Se revisa los paquetes con los que ingresan o salen los visitantes?

17. ¿Existe algún espacio físico para encargo de paquetes no autorizados el ingreso o para abrir la salida de los mismos si es el caso?

18. ¿Existe Políticas de Seguridad de la Información?
19. ¿Existe un Plan Estratégico para el control de los Bienes Muebles e Inmuebles?
20. ¿Qué tipo de sistema utiliza para automatizar la información?
21. ¿Cuentan con un Sistema de Control de Inventarios?

Encuesta Unidad Talento Humano

1. ¿Qué tipo de políticas aplican para la contratación del talento humano?
2. ¿Se verifica el desenvolvimiento en actividades asignadas del talento humano en otros trabajos antes de contratar?
3. ¿Se respeta los roles y funciones para lo que fueron contratados?
4. ¿Existen políticas de confiabilidad no divulgación de la información institucional?
5. ¿Existe un Plan estratégico para la administración de recursos humanos?
6. ¿En qué periodo de tiempo se realizan las contrataciones de un cargo es definido?
7. ¿El momento del cese de funciones del talento humano, tienen políticas para la entrega de la información, documentos y equipos de oficina que estaban bajo la responsabilidad del personal saliente?

Encuesta Unidad Técnica, Planificación, Financiera

1. ¿Se aplican políticas de seguridad para la información?
2. ¿De qué manera se realiza un control de la seguridad de la información?
3. ¿Describa el control interno informático que se realiza en la Unidad de Tecnologías?
4. ¿Conoce usted acerca de un Plan de seguridad de la información en el MTOP?.
5. ¿Qué mecanismo, técnicas y/o herramientas de seguridad se aplican en los sistemas de información y de comunicación?
6. ¿Se realiza control y administración de riesgos en cuanto a la seguridad de la información?
7. ¿Se realizan tareas de monitoreo a los sistemas de información y de comunicación?
8. ¿Han realizado simulacros frente a la caída de los sistemas de información y de comunicación?

9. ¿La información que contienen los sistemas Informáticos que son utilizados para la Administración de la información, es integra, confiable y veraz?

Encuesta Unidad Tecnológica.

Institución:			
Encuesta referente al Control Bases de Datos			
Dominio	Bases de Datos		
Proceso	Seguridad de la Información		
Objetivo de Control	Seguridad de la Información Bases de Datos		
Encuesta			
Pregunta	SI	NO	PORQUE
¿Existe algún archivo de tipo Log donde guarde información referida a las operaciones que realiza la Base de datos?			
¿Se realiza copias de seguridad (diariamente, semanalmente, Mensualmente, etc.)?			
¿Existe algún usuario que no sea el DBA pero que tenga asignado el rol DBA del servidor?			
¿Son gestionados los perfiles de los usuarios por el administrador?			
¿Se renuevan las claves de los usuarios de la Base de Datos?			
¿Se obliga el cambio de la contraseña de forma automática?			
¿Se encuentran listados de todos aquellos intentos de accesos no satisfactorios o denegados a estructuras, tablas físicas y lógicas del repositorio?			
¿Posee la base de datos un diseño físico y lógico?			
¿Los datos utilizados en el entorno de desarrollo, son reales?			
¿Las copias de seguridad se efectúan diariamente?			

¿Las copias de seguridad son encriptados?			
¿Se ha probado restaurar alguna vez una copia de seguridad, para probar que las mismas se encuentren bien hechas?			
¿Los dispositivos que tienen las copias de seguridad, son almacenados fuera del edificio de la institución?			
¿En caso de que el equipo principal sufra una avería, existen equipos auxiliares?			
¿Cuándo se necesita restablecer la base de datos, se le comunica al administrador?			
¿Se lleva a cabo una comprobación, para verificar que los cambios efectuados son los solicitados por el interesado?			
¿Se documentan los cambios efectuados?			
¿El motor de Base de Datos soporta herramientas de auditoría?			
¿Existe algún plan de contingencia ante alguna situación no deseada en la Base de Datos?			
Documentos probatorios presentados:			
TOTAL			

Institución:			
Encuesta para el Control Inventario			
Dominio	Redes y Comunicaciones		
Proceso	Seguridad de la Información		
Objetivo de Control Evaluación Infraestructura de las redes			
Encuesta			
Preguntas	SI	NO	PORQUE
¿Los nodos se encuentran bajo un mismo estándar, para evitar la reducción de la velocidad de transmisión?			
¿La infraestructura de la red inalámbrica se gestiona en base a los recursos de radiofrecuencia?			
¿Se testean los enlaces de red con frecuencia?			

¿La longitud de los tramos de cableado horizontal no excede de los 90 metros?			
¿Para el armado del patch panel se considera el cumplimiento de los requerimientos básicos establecidos en normas de seguridad?			
¿Se implementa códigos de colores para el etiquetado de la institución para facilitar su identificación?			
¿Existe canaletas o ductos para el cableado estructurado?			
¿Existe dispositivo firewall para protección de la red?			
¿Las direcciones IPS son fijas?			
¿Para la expansión de redes locales, tienen conmutadores en red?			
¿Existe un sistema de control de acceso a dispositivos del cableado de red?			
¿Para el funcionamiento de la red existe un plan de contingencia?			
¿En la configuración de dispositivos se analiza las posibles vulnerabilidades?			
¿Se realiza pruebas de cableado para probar la solidez de la red y encontrar posibles fallas?			
¿Cuentan con administración interna de la red para la administración en cada oficina?			
¿Usan protocolos de autenticación, para evitar vulnerabilidades?			
¿Los dispositivos Access Point es la cantidad adecuada en función del número de servidores?			
Documentos probatorios presentados:			

TOTAL			

Institución:			
Encuesta para el Control Inventario			
Dominio	Adquirir y mantener la arquitectura tecnológica		
Proceso	Seguridad de la Información.		
Objetivo de Control	Seguridad de la Información		
Encuesta			
Pregunta	SI	NO	PORQUE?
¿Se cuenta con un inventario trimestral de todos los equipos que integran el centro de cómputo del MTOP?			
¿Se posee de bitácoras de fallas detectadas en los equipos?			
CARACTERISTICAS DE LA BITACORA (SEÑALE LAS OPCIONES).			
¿La bitácora es llenada por personal especializado?			
¿Señala fecha de detección de la falla?			
¿Señala fecha de corrección de la falla y revisión de que el equipo funcione correctamente?			

Institución:	
Encuesta de Control y seguridad Instalaciones y Cubículos	
Dominio	Administración de Instalaciones.

Proceso	Seguridad de la Información.
Objetivo de Control	Instalaciones, adecuaciones y seguridad

Encuesta

Pregunta	SI	NO	PORQUE
¿Las instalaciones (cubículos y oficinas) fueron diseñadas específicamente para funcionar como un centro de cómputo?			
¿Existen lugares de acceso restringido?			
¿Se cuenta con sistemas de seguridad para impedir el paso a lugares de acceso restringido?			
¿Se cuenta con sistemas de emergencia como son detectores de humo, alarmas, u otro tipo de censores?			
¿Existen señalizaciones adecuadas en las salidas de emergencia y se tienen establecidas rutas de evacuación?			
¿Se cuenta con iluminación adecuada y con iluminación de emergencia en casos de contingencia?			
¿Se tienen sistemas de seguridad para evitar que se sustraiga equipo de las instalaciones?			
¿Se tiene un lugar asignado para papelería y utensilios de trabajo?			
¿Existen prohibiciones para fumar, consumir alimentos y bebidas?			
¿Se realiza limpieza de los ductos de aire y la cámara de aire que existe debajo del piso falso (si existe)?			
Documentos probatorios presentados:			

Institución:	
Encuesta de Control Impacto Ambiental	
Dominio	Entrega de Servicios y Soportes
Proceso	Seguridad de la información contra Factores Ambientales
Objetivo de Control	Controles Ambientales

Encuesta			
Preguntas	SI	NO	PORQUE
¿El centro de cómputo tiene alguna sección con sistema de refrigeración?			
¿Con cuanta frecuencia se revisan y calibran los controles ambientales?			
¿Se tiene contrato de mantenimiento para los equipos que proporcionan el control ambiental?			
¿Se tienen instalados y se limpian regularmente los filtros de aire?			
¿Con cuanta frecuencia se limpian los filtros de aire?			
¿Se tiene plan de contingencia en caso de que fallen los controles ambientales? ¿Se cuenta con políticas claras y definidas al finalizar la vida útil de los elementos informáticos que se dan de baja?			

Documentos probatorios presentados:

TOTAL

Institución:	
Encuesta de Control Respaldo Eléctrico	
Dominio	Entrega de Servicios y Soportes
Proceso	Seguridad de la Información
Objetivo de Control	Suministro Ininterrumpido de Energía

Encuesta			
Pregunta	SI	NO	PORQUE
¿Existe instalación a tierra para los equipos tecnológicos?			

¿Las instalaciones eléctricas se implementaron de manera especial para el centro tecnológico?			
¿Se cuenta con un tablero de distribución?			
¿El tablero de distribución se encuentra en un lugar accesible?			
¿El tablero considera espacio para futuras ampliaciones del centro tecnológico?			
¿Las instalaciones eléctricas son diferentes para el centro tecnológico?			
¿La instalación eléctrica para el centro tecnológica es la misma para la iluminación de todo el edificio?			
¿Existe ventiladores y aire acondicionado que estén conectados la misma instalación de los equipos?			
¿Se cuenta con una instalación de interruptores generales?			
¿Existe interruptores de emergencia?			
¿Los interruptores se rotulan conforme a códigos tecnológicos establecidos?			
¿Existe implementado medios de seguridad ante un corto circuito?			
¿Existe equipo de energía auxiliar?			
¿Se cuenta con Planta eléctrica para solventar de emergencia?			
Documentos probatorios presentados:			
TOTAL			

Institución:	
Encuesta de Control Seguridad Lógica e Tecnología	
Dominio	Manejo de Información y elementos
Proceso	Seguridad de la Información

Objetivo de Control	Seguridad de la Información		
Encuesta			
Pregunta	SI	NO	PORQUE
¿Existen metodologías de respaldo de información?			
¿Existen metodologías de respaldo de información, basados en las Normas ISO 27000?			
¿Existe un Plan Estratégico tecnológico Anual?			
Existe un administrador de sistemas que controle las cuentas de los usuarios?			
¿Existe algún estándar para la creación de contraseñas?			
¿Las contraseñas cuentan con letras, números y símbolos?			
¿Se obliga, cada cierto tiempo a cambiar la contraseña?			
¿La organización cuenta con un proceso para dar mantenimiento preventivo y correctivo al software?			
¿La organización cuenta con un proceso para dar mantenimiento preventivo y correctivo al hardware, maquinarias y otros equipos tecnológicos?			
¿Se tienen software antivirus instalados y actualizados en los equipos de cómputo?			
¿Se tienen instalados anti malware en los equipos de cómputo?			
¿Cuenta con licencias de software?			
¿Existe un proceso para adquirir y mantener las licencias actualizadas?			
¿Se sanciona al integrante del departamento si instala software no permitido?			
¿Los usuarios de bajo nivel tienen restringido el acceso a las partes más delicadas de las aplicaciones?			
¿El equipo de cómputo cuenta con suficiente espacio en HD en función de los servicios que otorga?			
¿El equipo de cómputo cuenta con suficiente memoria RAM en función de los servicios que otorga?			
¿La velocidad del procesador es el adecuado para los programas que son utilizados en los equipos?			
Documentos probatorios presentados:			
TOTAL			

¿Es considerada la maquinaria pesada, equipo caminero y otros tipos de equipos que utilizan para realizar las actividades del Ministerio de Transporte y Obras Públicas, como parte del equipo tecnológico de la institución, para realizar su respectiva administración?

Apéndice B

Resultado de Encuestas.

Tabla: Respuesta encuesta Unidad Talento Humano

PREGUNTA	RESPUESTA 1	RESPUESTA 2	RESPUESTA 3	RESPUESTA 4	PUNTAJE
¿Qué tipo de políticas aplican para la contratación del talento humano?	La ley de la LOSEP	perfiles del puesto	Necesidades de la institución.	Se contrata por petición de autoridades	16
¿Se verifica el desenvolvimiento en actividades asignadas del talento humano en otros trabajos antes de contratar?	se solicita certificaciones	se solicita 3 certificaciones	se solicita certificaciones	se solicita certificaciones	12
¿Se respeta los roles y funciones para lo que fueron contratados?	no realizan diferentes actividades	si	si pero hacen actividades extras	conforme a disposiciones de autoridades	8
¿Existen políticas de confiabilidad no divulgación de la información institucional?	si acuerdo de confiabilidad	si no pueden divulgar la información	acuerdo de confiabilidad	acuerdo de confiabilidad	12
¿Existe un Plan estratégico para la administración de recursos humanos?	no	no	no	No	0
¿En qué periodo de tiempo se realizan las contrataciones de un cargo es definido?	no	cada 2 años	no	No	0

El momento del cese de funciones del talento humano, tienen políticas para la entrega de la información, documentos y equipos de oficina que estaban bajo la responsabilidad del personal saliente.	Entregan los bienes y documentos para entregar un certificado de bodega e informe de talento humano para la liquidación.	Entregan equipo de oficina	No entregan informe	Si entregan todo para realizar la liquidación.	14
				TOTAL	**62/140**
				PORCENTAJE	**44,29**

Fuente: Elaboración propia.

Tabla: Respuesta encuesta Unidad Tecnología.

Encuesta referente al Control Bases de Datos				
Pregunta	**Si**	**NO**	**PORQUE**	**PUNTAJE**
¿Existe algún archivo de tipo Log donde guarde información referida a las operaciones que realiza la Base de datos?	6	2		30
¿Se realiza copias de seguridad (diariamente, semanalmente, Mensualmente, etc.)?	8	0		40
¿Existe algún usuario que no sea el DBA pero que tenga asignado el rol DBA del servidor?	1	7	Solo hay un administrador	5
¿Son gestionados los perfiles de los usuarios por el administrador?	4	4	Hay personal asignada.	20
¿Se renuevan las claves de los usuarios de la Base de Datos?	8	0		40
¿Se obliga el cambio de la contraseña de forma automática?	5	3	Uno se solicita	25
¿Se encuentran listados de todos aquellos intentos de accesos no satisfactorios o denegados a estructuras, tablas físicas y lógicas del repositorio?	7	1	No existe bitácoras	35
¿Posee la base de datos un diseño físico y lógico?	8	0		40
¿Los datos utilizados en el entorno de desarrollo, son reales?	5	3		25

¿Las copias de seguridad se efectúan diariamente?	4	4		20
¿Las copias de seguridad son encriptados?	2	6		10
¿Se ha probado restaurar alguna vez una copia de seguridad, para probar que las mismas se encuentren bien hechas?	4	4		20
¿Los dispositivos que tienen las copias de seguridad, son almacenados fuera del edificio de la institución?	5	7	en la nube	25
¿En caso de que el equipo principal sufra una avería, existen equipos auxiliares?	7	1		35
¿Cuándo se necesita restablecer la base de datos, se le comunica al administrador?	3	5	Hay sistemas que son manejados por otra institución.	15
¿Se lleva a cabo una comprobación, para verificar que los cambios efectuados son los solicitados por el interesado?	3	5		15
¿Se documentan los cambios efectuados?	4	4	En el código	20
¿El motor de Base de Datos soporta herramientas de auditoría?	4	4		20
¿Existe algún plan de contingencia ante alguna situación no deseada en la Base de Datos?	4	4		20
TOTAL				**460/760**
PORCENTAJE				**60,53**
Encuesta para el Control Inventario				
¿Los nodos se encuentran bajo un mismo estándar, para evitar la reducción de la velocidad de transmisión?	4	6		20
¿La infraestructura de la red inalámbrica se gestiona en base a los recursos de radiofrecuencia?	4	6		20
¿Se testean los enlaces de red con frecuencia?	6	4		30
¿La longitud de los tramos de cableado horizontal no excede de los 90 metros?	4	6		20
¿Para el armado del patch panel se considera el cumplimiento de los requerimientos básicos establecidos en normas de seguridad?	4	6		20
¿Se implementa códigos de colores para el etiquetado de la institución para facilitar su identificación?	5	5		25
¿Existe canaletas o ductos para el cableado estructurado?	10	0		50
¿Existe dispositivo firewall para protección de la red?	8	2		40
¿Las direcciones IPS son fijas?	4	6		20
¿Para la expansión de redes locales, tienen conmutadores en red?	6	4		30

¿Existe un sistema de control de acceso a dispositivos del cableado de red?	4	6		20
¿Para el funcionamiento de la red existe un plan de contingencia?	3	7		15
¿En la configuración de dispositivos se analiza las posibles vulnerabilidades?	3	7	Se contrató técnicos para la	15
¿Se realiza pruebas de cableado para probar la solidez de la red y encontrar posibles fallas?	4	6		20
¿Cuentan con administración interna de la red para la administración en cada oficina?	3	7		15
¿Usan protocolos de autenticación, para evitar vulnerabilidades?	2	8		10
¿Los dispositivos Access Point es la cantidad adecuada en función del número de servidores?	4	6		20
¿Se cuenta con un inventario trimestral de todos los equipos que integran el centro de cómputo del MTOP?	2	8		10
¿Se posee de bitácoras de fallas detectadas en los equipos?	1	9		5
¿La bitácora es llenada por personal especializado?	2	8		10
¿Señala fecha de detección de la falla?	3	7		15
¿Señala fecha de corrección de la falla y revisión de que el equipo funcione correctamente?	2	8		10
TOTAL				440/1100
PORCENTAJE				40
Encuesta de Control y seguridad Instalaciones y Cubículos				
¿Las instalaciones (cubículos y oficinas) fueron diseñadas específicamente para funcionar como un centro de cómputo?	2	8		10
¿Existen lugares de acceso restringido?	4	6		20
¿Se cuenta con sistemas de seguridad para impedir el paso a lugares de acceso restringido?	3	7		15
¿Se cuenta con sistemas de emergencia como son detectores de humo, alarmas, u otro tipo de censores?	8	2		40
¿Existen señalizaciones adecuadas en las salidas de emergencia y se tienen establecidas rutas de evacuación?	3	7		15
¿Se cuenta con iluminación adecuada y con iluminación de emergencia en casos de contingencia?	4	6		20

¿Se tienen sistemas de seguridad para evitar que se sustraiga equipo de las instalaciones?	2	8		10
¿Se tiene un lugar asignado para papelería y utensilios de trabajo?	4	6		20
¿Existen prohibiciones para fumar, consumir alimentos y bebidas?	1	9		5
¿Se realiza limpieza de los ductos de aire y la cámara de aire que existe debajo del piso falso (si existe)?		10		0
TOTAL				**155/500**
PORCENTAJE				**31**
Encuesta de Control Impacto Ambiental				
¿El centro de cómputo tiene alguna sección con sistema de refrigeración?	3	4		15
¿Se revisan y calibran los controles ambientales?	2	5		10
¿Se tiene contrato de mantenimiento para los equipos que proporcionan el control ambiental?	1	6		5
¿Se tienen instalados y se limpian regularmente los filtros de aire?	1	6		5
¿Se cuenta con políticas claras y definidas al finalizar la vida útil de los elementos informáticos que se dan de baja?	3	4		15
TOTAL				**50/175**
PORCENTAJE				**28,57**
Encuesta de Control Respaldo Eléctrico				
¿Existe instalación a tierra para los equipos tecnológicos?	10			50
¿Las instalaciones eléctricas se implementaron de manera especial para el centro tecnológico?	4	6		20
¿Se cuenta con un tablero de distribución?	10			50
¿El tablero de distribución se encuentra en un lugar accesible?	0	10		
¿El tablero considera espacio para futuras ampliaciones del centro tecnológico?	10	0		50
¿Las instalaciones eléctricas son diferentes para el centro tecnológico?	10	0		50

¿La instalación eléctrica para el centro tecnológica es la misma para la iluminación de todo el edificio?	0	10		10
¿Existe ventiladores y aire acondicionado que estén conectados la misma instalación de los equipos?	8	2		40
¿Se cuenta con una instalación de interruptores generales?	5	5		25
¿Existe interruptores de emergencia?	4	6		20
¿Los interruptores se rotulan conforme a códigos tecnológicos establecidos?	10			50
¿Existe implementado medios de seguridad ante un corto circuito?	10			50
¿Existe equipo de energía auxiliar?	9	1		45
¿Se cuenta con Planta eléctrica para solventar de emergencia?	4	6		20
TOTAL				480/750
PORCENTAJE				64
Encuesta de Control Seguridad Lógica e Tecnología				
¿Existen metodologías de respaldo de información?	7	5		35
¿Existen metodologías de respaldo de información, basados en las Normas ISO 27000?	4	8		20
¿Existe un Plan Estratégico tecnológico Anual?	4	8		20
¿Existe un administrador de sistemas que controle las cuentas de los usuarios?	2	10		10
¿Existe algún estándar para la creación de contraseñas?	5	7		25
¿Las contraseñas cuentan con letras, números y símbolos?	8	4	Depende de los sistemas	40
¿Se obliga, cada cierto tiempo a cambiar la contraseña?	2	10		10
¿La organización cuenta con un proceso para dar mantenimiento preventivo y correctivo al software?	4	8		20
¿La organización cuenta con un proceso para dar mantenimiento preventivo y correctivo al hardware, maquinarias y otros equipos tecnológicos?	4	8		20
¿Se tienen software antivirus instalados y actualizados en los equipos de cómputo?	12	0		60
¿Se tienen instalados anti malware en los equipos de cómputo?	0	12	Tienen incluido en el antivirus	0

¿Cuenta con licencias de software?	4	8		20
¿Existe un proceso para adquirir y mantener las licencias actualizadas?	2	10		10
¿Se sanciona al integrante del departamento si instala software no permitido?	0	12		0
¿Los usuarios de bajo nivel tienen restringido el acceso a las partes más delicadas de las aplicaciones?	6	6	No hay seguridades en las claves	30
¿El equipo de cómputo cuenta con suficiente espacio en HD en función de los servicios que otorga?	4	8		20
¿El equipo de cómputo cuenta con suficiente memoria RAM en función de los servicios que otorga?	7	5		35
¿La velocidad del procesador es el adecuado para los programas que son utilizados en los equipos?	7	5		35
TOTAL				410/1080
PORCENTAJE				37,96

Fuente: Elaboración propia.

Tabla: Respuesta encuesta Unidad Administrativa y Bodega.

PREGUNTA	RES 1	RES 2	RES 3	RES4	RES 5	PUNTAJE
¿Existe un Plan de Vigilancia implementado en el MTOP?	No ,se contrata servicio de vigilancia	No, la seguridad contratada	Si se contrata servicio de vigilancia en todo el país	No existe un plan	Se desconoce.	8
¿Existe alguna autorización permanente de estancia de personal ajeno a la institución?	Ninguno	Ninguno	Ninguno	Ninguno	Ninguno	0
¿Quiénes saben cuáles son las personas autorizadas de ingresar al MTOP?	No, todos pueden ingresar	No, hay acceso restringido	No, todos pueden ingresar	No, todos pueden ingresar	No, se puede control esto ya que se brinda servicios a	15

					los usuarios.	
4. Además de la tarjeta magnética de identificación, ¿hay otras especiales para los visitantes?	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	0
¿Se pregunta a los visitantes a que Unidad y a quien van visitar?	Si se realiza el registro con hora de ingreso y de salida.	Si se realiza el registro con hora de ingreso y de salida.	Si se realiza el registro con hora de ingreso y de salida.	Registro con hora de ingreso y de salida.	Si se realiza el registro con hora de ingreso y de salida.	20
¿Cómo se controla el horario de visitas?	El horario establecido de las 8 horas	No se tienen control porque algunos ingresan después del horario laboral.	En el horario establecido	Ninguno	Ninguno	9
¿Existe Controles Automáticos para el Ingreso al MTOP?	Ninguno	Ninguno	Ninguno	Ninguno	Ninguno	0
¿Quedan registradas todas las entradas y salidas al MTOP?	De manera manual	En una bitácora del guardia	Por los registros de seguridad.	En un cuaderno de forma manual	En el listado de los guardias.	15
Al final de cada turno, ¿Se controla el número de entradas y salidas del personal y visitas de la Institución?	No, cada guardia hace la entrega de turnos	Ninguno	Se desconoce	No, cada guardia entrega el cambio de turno	El guardia lleva la bitácora.	9

¿Puede salirse del MTOP sin registro alguno	El guardia registra salidas del personal u usuarios	Si porque a veces no está el guardia	Si	No porque se solicita permiso al superior	Se desconoce.	16
¿Existe vigilantes las 24 horas?	Si.	Si los guardias	Si los guardias	Si los guardias	Si los guardias	25
¿Existen cámaras de vigilancia?	Si pero no se monitorea	No	Si	Si	No	15
Identificadas las visitas, ¿Se les acompaña hasta la persona que desean ver?	Solo se informa en qué lugar les pueden localizar	No solo se registra el ingreso	Le informan donde le pueden localizar.	Le informan donde le pueden localizar.	Le informan donde le pueden localizar.	15
¿Qué tipo de control especial aplican en la vigilancia por la noche?	Ninguno	No se	Se desconoce	Ninguno	Se desconoce.	0
¿Existe una adecuada política de registros del personal y visitantes?	Es un registro manual	Se debería tener un sistema de control	Registro manual	Algunos no coincide el número de cedula	No existe un registro optimo	15
¿Se revisa los paquetes con los que ingresan o salen los visitantes?	No están autorizados los guardias	Ninguno	Ninguno	Ninguno	Ninguno	3
¿Existe algún espacio físico para encargo de paquetes no autorizados el ingreso o para abrir la salida de los mismos si es el caso?	No existe	No existe	No existe	No existe	No existe	0

¿Existe Políticas de Seguridad de la Información?	No	Ninguno	Los inventarios	El registro de los equipos que se conservan	Ninguno	7
¿Existe un Plan Estratégico para el control de los Bienes Muebles e Inmuebles?	Ninguno	Ninguno	Ninguno	Ninguno	Se está trabando en eso.	3
¿Qué tipo de sistema utiliza para automatizar la información?	Excel	Excel	Excel y SITOP	Excel	Excel	15
¿Cuentan con un Sistema de Control de Inventarios?	No existe	El modulo en el SITOP	No existe	No existe	No existe	4
TOTAL						**194/315**
PORCENTAJE						**61,58**

Fuente: Elaboración propia.

Tabla: Respuesta encuesta Unidades Financiero, Planificación, Técnico.

PREGUNTA	RES 1	RES 2	RES 3	RES 4	RES 5	RES 6	PUNTAJE
¿Se aplican políticas de seguridad para la información?	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	Ninguna	0
¿De qué manera se realiza un control de la seguridad de la información?	Si conforme al manejo del sistema Quipux.	Sistema Quipux	No, porque todos pueden ingresar al sistemas y buscar los documentos	Sistema Quipux	Sistema Quipux	Sistema Quipux	9

¿Describa el control interno informático que se realiza en la Unidad de Tecnologías?	No se tienen conocimiento.	Asignando claves y usuarios para manejar los sistemas.	No se tienen conocimiento.	Ninguno	Crean claves para cada técnico.	Activación de internet.	9
¿Conoce usted acerca de un Plan de seguridad de la información en el MTOP ?.	No se tienen conocimiento.	No se tienen conocimiento.	No se tienen conocimiento.	No se tienen conocimiento.	No se tienen conocimiento.	No se tienen conocimiento.	0
¿Qué mecanismo, técnicas y/o herramientas de seguridad se aplican en los sistemas de información y de comunicación?	Se desconoce	Se desconoce	Se desconoce	No se tienen acceso a toda la información.	Restringido el ingreso a sistemas informáticos.	Ninguno	8
¿Se realiza control y administración de riesgos en cuanto a la seguridad de la información?	Ninguno	No	Ninguno	No	No	No	0
¿Se realizan tareas de monitoreo a los sistemas de información y de comunicación?	Lo realizan los proveedores de los sistemas	No ninguno	No ninguno	No ninguno	No ninguno	No ninguno	3
¿Han realizado simulacros frente a la caída de los sistemas de información y de comunicación?	Ninguno	No	Ninguno	Ninguno	Ninguno	Ninguno	3
¿La información que contienen los sistemas Informáticos que son utilizados para la Administración de la información, es integra, confiable y veraz?	No porque cada vez piden que se envié la información de manera manual a los técnicos	Solicitan que se llene la información en matrices y no se genere de los sistemas	Siempre solicitan información actualizada.	La información es actualizada Mensualmente pero presenta fallas en el sistema.	Existen fallas en el sistema que no permite que la información sea verídica.	Implementación de módulos sin relacionarse con las informaciones correspondientes.	18
						TOTAL	**50/270**

PORCENTAJE	**18,51**

Fuente: Elaboración propia.

Tabla: Respuesta encuesta Unidades Archivo y Secretaria.

PREGUNTAS	RES 1	RES 2	RES 3	PUNTAJE
¿Existe Políticas de Seguridad de la Información?	No, porque no tiene las seguridades correspondientes	Si, conforme a lo estipulado por la secretaria de control de archivos.	Si con las normativas establecidas del MTOP.	10
¿Existe un Plan Estratégico para el control de los Archivos?	Ninguno	Ninguno	Ninguno	0
¿Qué tipo de sistema utiliza para automatizar la información?	Excel	Excel	Excel	3
¿Cuentan con un Sistema de Control de Archivos?	Normas establecidas	Técnicas de archivo	Ninguna	10
¿Existen Normas para la conservación de los documentos de Archivo?	Normas internas	Ninguna	Técnicas generales.	10
			TOTAL	**33/75**
			PORCENTAJE	**44**

Fuente: Elaboración propia.

Apéndice C

Análisis de Riesgos

Tabla: Matriz de riesgos Unidad de Secretaria y Archivo.

Ministerio de Transporte y Obras Públicas		MATRIZ DE RIESGOS PROCESO DE PLAN DE SEGURIDAD DE LA INFORMACIÒN			
(1) CÓDIGO		1	2	3	4
(2) RIESGO		Carecen de políticas de seguridad de la información propias del MTOP	Falta de aplicación de normativas conforme a Acuerdo 008-CG-2013	Carecen de un Plan estratégico para control de archivos	Falta de automatización de archivos
(3) DESCRIPCIÓN		Aplicar políticas de seguridad basadas en reglamentos emitidos a nivel nacional y no institucional.	Aplicar normativas conforme a acuerdos emitidos por otras entidades.	Deficiencia en elaboración de Plan estratégico	Utilizar solo la herramienta de Excel básico de office para la automatización
(4) CAUSAS		Reglamento emitido por otras entidades, Desconocimiento de tipo de políticas	Notificación de la aplicación del reglamento Falta de seguimiento.	No existe Plan estratégico Desconocimiento de cómo elaborarlo	las entidades públicas no pueden adquirir software el personal de sistemas no se abastece para el diseño de los mismos
(5) CONSECUENCIAS		Desorganización de documentos. Perdida de información.	Toma de decisiones no adecuadas	Manejo de información errónea, falencias en el proceso de archivología.	Informaciòn no actualizada, pérdida de tiempo en búsqueda de documentos de manera manual.
ANÁLISIS DE RIESGOS	**(6) VALOR**	15	10	20	20
	(7) PROBABILIDAD	Alta	Media	Alta	Alta
	(8) VALOR	3	2	2	2
	(9) IMPACTO	Catastrófico	Moderado	Moderado	Moderado
	(10) SEVERIDAD (Riego Inherente)	40	20	20	20
EVALUACIÓN DE RIESGOS	**(11) CONTROL**	Evaluación de experto	Divulgación de nuevas normativas, elaboración de propias reglas	Alternativas de elaboración de Plan Estratégico documental	Evaluación de experto, diseño de Sistema de gestión de Archivos.

			de manejo de documentación, monitoreo de cumplimiento.		
	(12) DESCRIPCIÓN DEL CONTROL	Diagnóstico de ventajas de aplicación de políticas	Monitoreo a la aplicación de normativas	Fortalecimiento de los procesos de control de archivos	Verificación de falencias de información no automatizada, Requerimientos para desarrollo del sistema de gestión.
	(13) TIPO DE CONTROL	Correctivo	Preventivo	Preventivo	Preventivo
	(14) ESTA DOCUMENTADO	Si	Si	Si	Si
	(15) DONDE ESTA DOCUMENTADO	Plan de seguridad de la información	Plan de seguridad de la información	Plan de seguridad de la información	Plan de seguridad de la información
	(16) APLICACIÓN	Si	Si	Si	Si
	(17) EFICACIA DEL CONTROL	Alta	Alta	Alta	Alta
	(18) FRECUENCIA DEL CONTROL	Anual	Diario	Anual	Según Ocurrencia
CALIFICACIÒN DE RIESGO RESIDUAL	**(19) VALOR**	5	10	10	10
	(20) PROBABILIDAD	Baja	Media	Media	Media
	(21) VALOR	2	2	2	2
	(22) IMPACTO	Moderado	Moderado	Moderado	Moderado
	(23) SEVERIDAD	10	20	20	20
TRATAMIENTO	**(24) ACCIÓN DE TRATAMIENTO**	Considerar la participación de la(s) persona experta	Socialización de las políticas y normativas del manejo documental	Reasignación de personal para elaboración de plan estratégico.	Aplicar buenas prácticas en el acceso a la información y desarrollo del sistema de gestión de archivos
	(25) TIEMPO DE IMPLEMENTACIÓN	Conforme aprobación del plan de seguridad de la información.	Conforme aprobación del plan de seguridad de la información.	Conforme aprobación del plan de seguridad de la información.	Conforme aprobación del plan de seguridad de la información.
	(26) COSTO	Medio	Medio	Medio	Medio
	(27) RESPONSABLE	Ministra, Asistente Administrativo Y procesos involucrados	Ministra, Asistente Administrativo Y procesos involucrados	Ministra, Asistente Administrativo Y procesos involucrados	Ministra, Asistente Administrativo, Unidad de Tecnológica Y procesos involucrados

Fuente: Elaboración propia.

Tabla: Matriz de riesgos Unidad de Bodega.

Ministerio de Transporte y Obras Públicas		MATRIZ DE RIESGOS PROCESO DE PLAN DE SEGURIDAD DE LA INFORMACIÒN		
(1) CÓDIGO		1	2	3
(2) RIESGO		Políticas de seguridad de la información de bodega	Plan estratégico de control de bienes	Automatización de inventario de bienes.
(3) DESCRIPCIÓN		Falta de elaboración de políticas de seguridad de bienes e información de bodega.	Carencia Plan estratégico de control de bienes	Falta de automatización de inventario de bienes.
(4) CAUSAS		Inadecuado control de bienes e información.	Informaciòn errónea, utilización de kardex de manera manual	Inadecuado control de inventario de bienes.
(5) CONSECUENCIAS		Perdida de bienes	Perdida de información	Incumplimiento con solicitud de información
ANÁLISIS DE RIESGOS	**(6) VALOR**	10	10	10
	(7) PROBABILIDAD	Media	Media	Media
	(8) VALOR	2	2	2
	(9) IMPACTO	Moderado	Moderado	Moderado
	(10) SEVERIDAD (Riego Inherente)	10	10	10
EVALUACIÓN DE RIESGOS	**(11) CONTROL**	Elaboración de un plan de seguridad de la información de los bienes de bodega.	Diseñar sistema de gestión interno de bienes	Diseño de un sistema de inventario
	(12) DESCRIPCIÓN DEL CONTROL	Definir las normas de seguridad para la confiabilidad de la información y bienes	Diagnóstico de requerimientos para cumplir con el sistema de gestión interno de bienes	Diagnóstico de requerimientos para cumplir con el sistema de inventario

	(13) TIPO DE CONTROL	Preventivo	Preventivo	Preventivo
	(14) ESTA DOCUMENTADO	Si	Si	Si
	(15) DONDE ESTA DOCUMENTADO	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciòn.
	(16) APLICACIÓN	Si	Si	Si
	(17) EFICACIA DEL CONTROL	Alta	Alta	Alta
	(18) FRECUENCIA DEL CONTROL	Anual	Semanal	Semanal
CALIFICACIÒN DE RIESGO RESIDUAL	**(19) VALOR**	10	10	10
	(20) PROBABILIDAD	Media	Media	Media
	(21) VALOR	2	2	2
	(22) IMPACTO	Moderado	Moderado	Moderado
	(23) SEVERIDAD	20	20	20
TRATAMIENTO	**(24) ACCIÓN DE TRATAMIENTO**	Divulgación del plan	Designar tareas y controlar las responsabilidades de acuerdo a la elaboración	Designar tareas y controlar las responsabilidades de acuerdo a la elaboración
	(25) TIEMPO DE IMPLEMENTACIÓN	Anual	Mensual	Mensual
	(26) COSTO	Medio	Medio	Medio
	(27) RESPONSABLE	Administrativo -Unidad de Tecnología	Administrativo-Unidad de Tecnología	Administrativo-Unidad de Tecnología

Fuente: Elaboración propia.

Tabla: Matriz de riesgos Unidad Administrativa.

Ministerio de Transporte y Obras Públicas	MATRIZ DE RIESGOS PROCESO DE PLAN DE SEGURIDAD DE LA INFORMACIÒN										
(1) CÓDIGO	1	2	3	4	5	6	7	8	9	10	11
(2) RIESGO	Contrato de servicio de vigilancia Anual	Acceso no autorizados a las instalaciones	Registro de visitantes	Verificación de los servidores si se encuentran en las instalaciones	Horario de visitas	Control de horario del personal	Registro ingresos y salidas visitantes y personal	Bitácoras de registros	Monitoreo cámaras de vigilancia	Carencia de control de seguridad en las noches	Plan organizacional para control de visitas y servidores
(3) DESCRIPCIÓN	Cambio de servicio de vigilancia de seguridad Anual	No existe restricción de acceso	registro de visitantes de manera manual	No se verifica si la persona a quien buscan está en la institución	No tienen un horario establecido	Solo se registra en el biométrico ingreso y salida del trabajo y lunch de los servidores.	No se registra todo los ingresos y salidas.	Solo hacen la entrega de los registros entre guardias.	Los Guardias No tienen opción a monitorear las cámaras de vigilancia.	No existe un control adecuado de seguridad en las noches	Falta de un plan organizacional para un control adecuado de las visitas de usuarios a la institución
(4) CAUSAS	Conforme a la ley se tiene que realizar Anualmente las contrataciones de servicio de vigilancia. No poseen normas de seguridad que deberían sujetarse el servicio de seguridad.	Ingreso de todas las personas incluyendo vendedores.	Falta de un registro automatizado para el registro de visitantes	Falta de medios de comunicación	Ingreso de visitantes fuera de horario de oficina	Falta de control automatizado de salida e ingreso de servidores en horario de trabajo.	Falta de un sistema de registro de visitantes	No se presenta un informe diario al administrador del control de ingreso y salida de personas	Falta de equipos de computo	Solo resguardan la parte interior	Falta de un Plan Organizacional

(5) CONSECUENCIAS		Aplicación de normas de cada empresa de seguridad al contratar	Falta de control del personal de vigilancia y aplicación de normas de seguridad internas del MTOP.	Registran de manera Manual en un cuaderno	No tienen teléfonos para comunicarse con el servidor a visitar para permitir el ingreso	No respetan horarios de oficina	Registran de manera Manual en un cuaderno	El guardia no siempre registra a todas las personas porque no está en su lugar de trabajo	El encargado de la Administración no solicita el informe diario de vigilancia	No pueden vigilar por medio de las cámaras de seguridad por falta de equipo de cómputo.	No hay un mecanismo de vigilancia de la parte exterior de las instalaciones.	Desorganización en proceso de vigilancia.
ANÁLISIS DE RIESGOS	**(6) VALOR**	10	20	20	20	10	20	10	20	20	20	20
	(7) PROBABILIDAD	Media	Alta	Alta	Alta	Media	Alta	Media	Alta	Alta	Alta	Alta
	(8) VALOR	2	3	3	3	2	3	2	3	3	3	3
	(9) IMPACTO	Moderado	Catastrófico	Catastrófico	Catastrófico	Moderado	Catastrófico	Moderado	Catastrófico	Catastrófico	Catastrófico	Catastrófico
	(10) SEVERIDAD (Riego Inherente)	20	60	60	60	20	60	20	60	60	60	60
EVALUACIÓN DE RIESGOS	**(11) CONTROL**	Realizar normas de control interno de vigilancia.	Determinar tipos de restricción de accesos.	Sistema de Registro de visitantes.	Evaluación administrativa	Establecer políticas de horario de visita	Establecer políticas de horario de trabajo de servidores.	Establecer políticas de seguridad.	Evaluación administrativa de bitácoras.	Implementación del Sistema de cámaras.	Evaluación administrativa.	Evaluación de experto
	(12) DESCRIPCIÓN DEL CONTROL	Elaboración de Normas de Control Interno. En los TDR'S de contratación determinar las normas	Elaboración de Normas de Control Interno, en el mismo que se clasifique el tipo de	Elaboración de un registro automatizado, Entrega de un equipo de cómputo.	Determinar la necesidad de un teléfono para comunicarse y verificar la presencia de los	Definir los horarios de vistas conforme a jerarquía institucional.	Elaboración de políticas de horario de los servidores semanalmente.	Instalación de puertas eléctricas para retener el ingreso de las personas que no han sido registradas, Elaboración	Informe diario de las bitácoras de los guardias.	Monitoreo de las cámaras de vigilancia, implementación de un equipo de cómputo.	Definir medios de seguridad para que los guardias tengan acceso a la parte exterior del edificio.	Definir las políticas de seguridad de activos para la elaboración de un plan organizacional.

		de control interno.	personas a ingresar y el acceso.		servidores.			de tarjeta de visitantes.				
	(13) TIPO DE CONTROL	Preventivo	Preventivo	Preventivo	Preventivo	Preventivo	Preventivo	Preventivo	Preventivo	Preventivo	Preventivo	Preventivo
	(14) ESTA DOCUMENTADO	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
	(15) DONDE ESTA DOCUMENTADO	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciòn.
	(16) APLICACIÓN	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
	(17) EFICACIA DEL CONTROL	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta
	(18) FRECUENCIA DEL CONTROL	Anual	Anual	Diariamente	Programado	Semanal	Semanal	Programado	Diariamente	Diariamente	Diariamente	Anual
CALIFICACIÒN DE RIESGO RESIDUAL	**(19) VALOR**	10	10	10	10	10	10	10	10	10	10	10
	(20) PROBABILIDAD	Media	Media	Media	Media	Media	Media	Media	Media	Media	Media	Media
	(21) VALOR	2	2	2	2	2	2	2	2	2	2	2
	(22) IMPACTO	Moderado	Moderado	Moderado	Moderado	Moderado	Moderado	Moderado	Moderado	Moderado	Moderado	Moderado
	(23) SEVERIDAD	20	20	20	20	20	20	20	20	20	20	20
TRATAMIENTO	**(24) ACCIÓN DE TRATAMIENTO**	Divulgación de las normas internas de seguridad.	Divulgación de las normas internas de seguridad.	Diseño de un sistema de registro u hoja de Cálculo Excel.	Permitir la colocación de in teléfono con IP, para la comunicación de los guardias con las	Divulgación de las normas internas de seguridad, referente a horarios	Divulgación de las normas internas de seguridad, referente a horarios establecidos, para el personal.	Permitir la implementación de una puerta eléctrica.	Presentación obligatoria diariamente del informe de bitácoras.	Permitir que los guardias monitoreen las cámaras de seguridad	Permitir la participación del experto para evaluar el la seguridad para el acceso	Permitir la participación del experto para elaborar el plan organizacional.

					personas a visitar.	establecidos.					exterior.	
	(25) TIEMPO DE IMPLEMENTACIÓN	Anual	Anual	Anual	Según la ocurrencia	Diariamente	Diariamente	Según la ocurrencia	Diariamente	Diariamente	Diariamente	Anual
	(26) COSTO	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio
	(27) RESPONSABLE	Bienes y suministros-Unidad de Tecnología - Vigilancia Externa-Servicios generales	Bienes y suministros-Unidad de Tecnología - Vigilancia Externa-Servicios generales	Bienes y suministros-Unidad de Tecnología - Vigilancia Externa-Servicios generales	Bienes y suministros-Unidad de Tecnología - Vigilancia Externa-Servicios generales	Bienes y suministros-Unidad de Tecnología - Vigilancia Externa-Servicios generales	Bienes y suministros-Unidad de Tecnología - Vigilancia Externa-Servicios generales	Bienes y suministros-Unidad de Tecnología - Vigilancia Externa-Servicios generales	Bienes y suministros-Unidad de Tecnología - Vigilancia Externa-Servicios generales	Bienes y suministros-Unidad de Tecnología - Vigilancia Externa-Servicios generales	Bienes y suministros-Unidad de Tecnología - Vigilancia Externa-Servicios generales	Bienes y suministros-Unidad de Tecnología - Vigilancia Externa-Servicios generales

Fuente: Elaboración propia.

Tabla: Matriz de riesgos Unidad Financiero, Planificación, Técnica.

MATRIZ DE RIESGOS PROCESO DE PLAN DE SEGURIDAD DE LA INFORMACIÒN

(1) CÓDIGO	1	2	3	4	5	6	7	8
(2) RIESGO	Falta de políticas de seguridad	Control interno de la Unidad de tecnología	Desconocimiento de un Plan de Seguridad de la Información	Control de seguridad en los sistemas informáticos.	Identificación de riesgos en la seguridad de la información	Monitoreo constante en los sistemas de información y comunicación	Carecen de alternativas de salvaguardar la información ante la caída de los sistemas de información.	Informaciòn no confiable
(3) DESCRIPCIÓN	La no aplicación de políticas de seguridad	Controles inadecuados de la Unidad de Tecnología	La no aplicación de un Plan de Seguridad de la Informaciòn	Aplicación inadecuado de seguridades al acceso de la información	La no realización de análisis de riesgos	La no constancia en monitoreo de los sistemas de información y comunicación.	Soluciones inadecuadas de salvaguardar la información.	La información no es integra, confiable.
(4) CAUSAS	Desconocimiento de las políticas de manejo de información.	Acceso no autorizado a información. Falta de cultura de tecnológica	Falta de aplicación de normas para salvaguardar la información	Bajo nivel de seguridad para el acceso a la información.	La inobservancia de los riesgos	Falta de actualización de la información, Desconocimiento de manejo de los sistemas de información. Falta de cultura tecnológica.	Falta de prevención para evitar pérdidas de información	Informaciòn desactualizada, Falta de documentación de respaldo
(5) CONSECUENCIAS	Perdida de información, toma de decisiones inadecuadas	Informaciòn errónea, fuga de información	Perdida de información, demora en los procesos, información	Perdida de información, información inoportuna,	Incumplimiento de procesos	Informaciòn errónea, accesos no autorizados	Informaciòn inoportuna fuera de fecha de	Demora en los procesos, pérdida de credibilidad

				inoportuna, Incumplimiento de los procesos.	Incumplimiento de proceso, alteración de la operaciones administrativas			proceso, respaldos inadecuados	de la imagen de la entidad ante el público,
ANÁLISIS DE RIESGOS	**(6) VALOR**	20	20	20	20	20	20	20	20
	(7) PROBABILIDAD	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta
	(8) VALOR	3	3	3	3	3	3	3	3
	(9) IMPACTO	Catastrófico	Catastrófico	Catastrófico	Catastrófico	Catastrófico	Catastrófico	Catastrófico	Catastrófico
	(10) SEVERIDAD (Riego Inherente)	60	60	60	60	60	60	60	60
EVALUACIÓN DE RIESGOS	**(11) CONTROL**	Evaluación de experto	Elaboración de plan de control interno	Diseño de un Plan de Seguridad de la Informaciòn	Diseño adecuado de acceso de usuarios	Diseño de un Plan de Seguridad de la Informaciòn que analice los riesgos	Plan de capacitaciones, determinar personal autorizado	Clasificación de categoría de importancia de la información para salvaguardar	Actualización semanal de la información, capacitación de personal.
	(12) DESCRIPCIÓN DEL CONTROL	Diagnóstico de tipo de políticas de seguridad aplicar	Determinar en el plan estratégico tecnológico, alternativas de un	Elaborar con expertos el Plan de Seguridad de la información	Generación de claves para trabajos individuales	Elaboración de un Plan de seguridad de la Informaciòn	Divulgación de responsabilidades y tareas	Definición de la importancia de la información	Generación de reportes semanales para confiabilidad de la

			control interno						información
	(13) TIPO DE CONTROL	Preventivo	Preventivo	Preventivo	Preventivo	Preventivo	Preventivo	Preventivo	Preventivo
	(14) ESTA DOCUMENTADO	Si	Si	Si	Si	Si	Si	Si	Si
	(15) DONDE ESTA DOCUMENTADO	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciòn.
	(16) APLICACIÓN	Si	Si	Si	Si	Si	Si	Si	Si
	(17) EFICACIA DEL CONTROL	Alta	Alta	Alta	Alta	Alta	Alta	Alta	Alta
	(18) FRECUENCIA DEL CONTROL	Anual	Mensual	Anual	Mensual	Anual	Mensual	Mensual	Semanal
CALIFICACIÒN DE RIESGO RESIDUAL	**(19) VALOR**	5	5	5	5	5	5	5	5
	(20) PROBABILIDAD	Baja	Baja	Baja	Baja	Baja	Baja	Baja	Baja
	(21) VALOR	2	2	2	2	2	2	2	2
	(22) IMPACTO	Moderado	Moderado	Moderado	Moderado	Moderado	Moderado	Moderado	Moderado
	(23) SEVERIDAD	10	10	10	10	10	10	10	10

TRATAMIENTO	**(24) ACCIÓN DE TRATAMIENTO**	Permitir que el experto evalué	Designar responsables para la elaboración de un plan estratégico.	Permitir que el experto evalué	Determinar normas para la generación de claves de seguridad	Permitir que el experto evalué	Determinar los cursos a seguir conforme a necesidades y mejoras institucionales	Responsable de archivo tener organizada la información conforme a normativas.	Determinar los cursos a seguir conforme a necesidades y mejoras institucionales
	(25) TIEMPO DE IMPLEMENTACIÓN	Según la ocurrencia	Según la ocurrencia	Según la ocurrencia	Según la ocurrencia	Según la ocurrencia	Mensual	Mensual	Mensual
	(26) COSTO	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio
	(27) RESPONSABLE	Administrativo Unidad de informática-comunicaciones	Administrativo Unidad de informática-comunicaciones	Administrativo	Unidad de informática-comunicaciones	Administrativo	Talento Humano	Administrativo	Talento Humano

Fuente: Elaboración propia.

Tabla: Matriz de riesgos Unidad Talento Humano.

Ministerio de Transporte y Obras Públicas	**MATRIZ DE RIESGOS PROCESO DE PLAN DE SEGURIDAD DE LA INFORMACIÒN**					
(1) CÓDIGO	1	2	3	4	5	6

(2) **RIESGO**	Políticas de contratación	Cumplimiento de roles	Discreción de la información.	Plan estratégico de Talento Humano	Tiempo de contratación 2 años	Terminación de contrato en el MTOP
(3) **DESCRIPCIÓN**	No existe una política definida de contratación	Realizan diferentes roles para lo que fueron contratados.	No existe seguimiento de la política de discreción de la información.	No existe un plan estratégico de Talento Humano	Se contrata personal Cada 2 años	Se registra la entrega de equipos de oficina y certifican para la liquidación.
(4) **CAUSAS**	Personal no apto	Inadecuada Ejecución de actividades que no fueron contratados	Divulgación de información	Inadecuado manejo de procesos de contratación de personal	Falta de continuidad de trabajo en las actividades	No se solicita la entrega de la información que manejaba dicho servidor.
(5) **CONSECUENCIAS**	Incumplimiento de tareas asignadas. Retraso en la entrega de trabajos	Información no confiable. Tareas no satisfactorias.	Manipulación de información por personas externas, antes de dar a conocer	No se respeta los perfiles de los puestos.	Pérdida de tiempo en la culminación en los procesos de las tareas asignada	Perdida de información.

						s	
ANÁLISIS DE RIESGOS	**(6) VALOR**	20	20	20	20	20	20
	(7) PROBABILIDAD	Alta	Alta	Alta	Alta	Alta	Alta
	(8) VALOR	3	3	3	3	3	3
	(9) IMPACTO	Catastrófico	Catastrófico	Catastrófico	Catastrófico	Catastrófico	Catastrófico
	(10) SEVERIDAD (Riego Inherente)	60	60	60	60	60	60
EVALUACIÓN DE RIESGOS	**(11) CONTROL**	Reforzar las políticas de contratación	Evaluar por expertos	Reforzar el acceso a la información	Reforzar los procesos de contratación	Evaluar por expertos	Divulgación de Políticas de entrega de información cese de funciones

	(12) DESCRIPCIÓN DEL CONTROL	Elaborar políticas internas de contratación de personal que se basen en las leyes y necesidades internas.	Definir los perfiles a contratar conforme a las necesidad de la institución	Restricción de permisos de seguridad para el ingreso de la información.	Definir con exactitud los procesos de contratación incluyendo los perfiles.	Definir periodos largos de contratación de acuerdo a proyectos o actividades, de terminar periodos fijos en cargos de libre remoción.	Desarrollo de políticas de entrega de información en cese de funciones de un servidor.
	(13) TIPO DE CONTROL	Correctivo	Correctivo	Correctivo	Correctivo	Correctivo	Correctivo
	(14) ESTA DOCUMENTADO	Si	Si	Si	Si	Si	Si
	(15) DONDE ESTA DOCUMENTADO	Plan de seguridad de la Informaciòn.	Plan de seguridad de la Informaciòn.	Plan de seguridad de la Informaciòn.	Plan de seguridad de la Informaciòn.	Plan de seguridad de la Informaciòn.	Plan de seguridad de la Informaciòn.
	(16) APLICACIÓN	Si	Si	Si	Si	Si	Si
	(17) EFICACIA DEL CONTROL	Alta	Alta	Alta	Alta	Alta	Alta

	(18) FRECUENCIA DEL CONTROL	Anual	Anual	Diariamente	Anual	Anual	Anual
CALIFICACIÒN DE RIESGO RESIDUAL	**(19) VALOR**	10	10	10	10	10	10
	(20) PROBABILIDAD	Media	Media	Media	Media	Media	Media
	(21) VALOR	2	2	2	2	2	2
	(22) IMPACTO	Moderado	Moderado	Moderado	Moderado	Moderado	Moderado
	(23) SEVERIDAD	20	20	20	20	20	20
TRATAMIENTO	**(24) ACCIÓN DE TRATAMIENTO**	Involucrar en las políticas de contratación las leyes vigentes de LOSEP y código de trabajo	Realizar uniformé de análisis de puestos vacantes y determinar el perfil indispensable.	Robustecer el control de acceso a la información física y digital.	Involucrar al personal capacitado para la elaboración de los procesos de contratación	Permitir que expertos evalúen los periodos de contratación.	Divulgación de Plan
	(25) TIEMPO DE IMPLEMENTACIÓN	Anual	Anual	Semanal	Anual	Anual	Anual

	(26) COSTO	Medio	Medio	Medio	Medio	Medio	Medio
	(27) RESPONSABLE	Autoridades y Talento Humano	Autoridades y Talento Humano	Autoridades y Talento Humano	Autoridades y Talento Humano	Autoridades y Talento Humano	Autoridades y Talento Humano

Fuente: Elaboración propia.

Tabla: Matriz de riesgos unidad de Tecnología.

Ministerio de Transporte y Obras Públicas	**MATRIZ DE RIESGOS PROCESO DE PLAN DE SEGURIDAD DE LA INFORMACIÒN**							
(1) CÓDIGO	1	2	3	4	7	8	9	11
(2) RIESGO	Inadecuado desarrollo de software y adquisición de hardware	Mal uso de la información	Vulnerabilidad del sistema de información	Daños, deterioro o pérdida de los recursos tecnológicos	Fallas en las redes de telecomunicaciones y sistema eléctrico	Desconocimiento del Plan Estratégico	Fracaso de eventos programados	Accesos no autorizados a las instalaciones de la unidad tecnológica

(3) **DESCRIPCIÓN**	Desarrollar un software que no cumpla los requerimientos de las necesidades del MTOP- Adquirir activos de comunicación (sw, router, etc.) que no cumpla los requerimientos para cumplir con las actividades diarias-	Riesgos de acceso, manipulación, divulgación de información privilegiada.	Ingreso de manera fraudulenta a los sistema de información del MTOP, hurtar la información.	Fallas de los recursos tecnológicos, en su uso, y almacenamiento.	Posibilidad de fallas en las redes de telecomunicaciones o en el sistema eléctrico.	No existe un informe de gestión	Falta de cultura tecnológica para talleres virtuales.	Ingreso de personas no autorizadas para la manipulación de equipos tecnológicos
(4) **CAUSAS**	Inadecuada información de requerimiento y/o necesidades del software Desconocimiento	Bajo conocimiento de seguridad para el acceso a la información. Desconocimiento de las políticas de seguridad del manejo de información. Acceso no autorizado a información. 5. Fraude interno.	Bajo conocimiento de seguridad para el acceso a la información. Cortafuegos inadecuados. Desconocimiento en estándares para la implementación de seguridad en los sistemas de información.	Inadecuado mantenimiento de los recursos tecnológicos Recursos tecnológicos de baja Calidad. Inadecuado uso de los recursos tecnológicos Falta de protección de los recursos tecnológicos. Factores ambientales	Falta de disponibilidad del servicio por parte del proveedor Falta de mantenimiento de los equipos y redes Deterioro de las redes Falla en las comunicaciones. Falta de protección ante pico de voltajes y interrupción del fluido eléctrico no planificado	Elaboración inadecua de informe. Desconocimiento del PETI en la unidad de tecnología.	Falta de divulgación.	Inadecuado control de acceso a las instalaciones Puertas no aptas para la seguridad

(5) CONSECUENCIAS		Inversión económica inadecuada Suspensión de los sistemas de información. Inestabilidad en los procesos - fallas en la red.	Toma de decisiones no adecuadas.	Inversión económica inadecuada. Inestabilidad de los procesos. Filtro de información	Equipos obsoletos, desperdicio de los recursos tecnológicos	Perdida de información, demora en los procesos, perdidas de la imagen de la entidad ante el público, información inoportuna, Incumplimiento de procesos.	Desconocimiento.	Inversión económica inadecuada, incumplimiento con los técnicos	Daños, manipulación robos en la infraestructur tecnológica
ANÁLISIS DE RIESGOS	**(6) VALOR**	10	10	20	20	20	20	20	20
	(7) PROBABILIDAD	Media	Media	Alta	Alta	Alta	Alta	Alta	Alta
	(8) VALOR	2	2	2	2	2	3	2	3
	(9) IMPACTO	Moderado	Moderado	Moderado	Moderado	Moderado	Catastrófico	Moderado	Catastrófico
	(10) SEVERIDAD (Riego Inherente)	10	20	40	20	40	40	40	60
EVALUACIÓN DE RIESGOS	**(11) CONTROL**	Evaluación de experto	Divulgación de las políticas de seguridad de la información. Monitorear los sistemas de información. Asignación de roles y accesos a los sistemas de información.	Procesos de control para la detección de vulnerabilidades en los sistemas de información. Buenas prácticas para el desarrollo e implementación de sistemas de información seguros.	Verificación de la toma eléctrica.	Condiciones operativas de la ups	Cronograma de información.	Diseñar programa de talleres, Diseño adecuado de la logística.	Reforzar el acceso físico a las instalaciones de tecnología, observación permanente d la unidad

	(12) DESCRIPCIÓN DEL CONTROL	Diagnóstico de ventajas y desventajas del software desarrollado	Establecimiento de roles y optimización de los controles en los sistemas de información	Verificación de las políticas de protección funcionen correctamente.	Verificación de los puntos eléctricos, identificar fallas en el fluido que pueda afectar el funcionamiento de los recursos tecnológicos.	Mantenimiento de la ups	Involucrar a todas las instancias que suministran información	Divulgación de responsabilidades y tareas	Instalación de nuevas puertas y cerraduras, control de ingresos a las instalaciones de informática
	(13) TIPO DE CONTROL	Preventivo	Preventivo	Preventivo	Preventivo	Preventivo	Preventivo	Preventivo	Preventivo
	(14) ESTA DOCUMENTADO	Si	Si	Si	Si	Si	Si	Si	Si
	(15) DONDE ESTA DOCUMENTADO	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciòn.	Plan de Seguridad de la Informaciò
	(16) APLICACIÓN	Si	Si	Si	Si	Si	Si	Si	Si
	(17) EFICACIA DEL CONTROL	Alta	Alta	Alta	Alta	Alta	Alta	Media	Alta
	(18) FRECUENCIA DEL CONTROL	Cuando se presenta	Mensual	Diario	Semanal	Semanal	Cuando se presenta	Cuando se presenta	Semanal
CALIFICACIÒN DE RIESGO Residual	**(19) VALOR**	5	5	10	5	10	5	5	10
	(20) PROBABILIDAD	BAJA	BAJA	Media	BAJA	Media	BAJA	BAJA	Media
	(21) VALOR	2	2	2	2	2	1	2	2
	(22) IMPACTO	Moderado	Moderado	Moderado	Moderado	Moderado	LEVE	Moderado	Moderado

	(23) SEVERIDAD	10	10	20	10	20	5	10	2
TRATAMIENTO	**(24) ACCIÓN DE TRATAMIENTO**	Permitir la participación de la(s) persona experta	Implementación de más niveles de seguridad.	Mejorar la seguridad de los cortafuegos. Aplicación de buenas prácticas en el desarrollo de sistemas de información seguros.	Controlar que los equipos institucionales tengan el antivirus institucional, el buen uso y su actualización	Mejorar las instalaciones eléctricas en la institución	Dar a conocer el plan estratégico tecnológico	Designar tareas y controlar las responsabilidades conforme a cronograma de talleres	Aplicar controles de acceso físico en la unidad
	(25) TIEMPO DE IMPLEMENTACIÓN	Según la ocurrencia	Según la ocurrencia	Diario	Semanal	Según la ocurrencia	Según la ocurrencia	Según la ocurrencia	Diario
	(26) COSTO	Bajo	Medio	Medio	Medio	Alto	Bajo	Medio	Medio
	(27) RESPONSABLE	Unidad de Tecnología	Unidad de Tecnología	Unidad de Tecnología	Unidad de Tecnología	Unidad de Tecnología	Unidad de Tecnología	Unidad de Tecnología	Unidad de Tecnología

Fuente: Elaboración propia.

Tabla: Riesgos y Normas ISO

UNIDAD	RIESGO	CONSECUENCIAS	NORMAS ISO 27002-DOMINIOS
ARCHIVO	Carecen de políticas de seguridad de la información propias del MTOP	Desorganización de documentos. Perdida de información.	GESTION DE ACTIVOS, POLITICAS DE LA SEGURIDAD DE LA INFORMACIÓN.
	Falta de aplicación de normativas conforme a Acuerdo 008-CG-2013	Toma de decisiones no adecuadas	
	Carecen de un Plan estratégico para control de archivos	Manejo de información errónea, falencias en el proceso de archivología.	
	Falta de automatización de archivos	Información no actualizada, pérdidas de tiempo en búsqueda de documentos de manera manual.	
PLANIFICACION, FINANCIERO, AREA TECNICA	Falta de políticas de seguridad	Perdida de información., toma de decisiones inadecuadas	POLITICAS DE LA SEGURIDAD DE LA INFORMACIÓN, GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
	Control interno de la Unidad de tecnología	Información errónea, fuga de información	
	Desconocimiento de un Plan de Seguridad de la Información	Perdida de información, retaso en los procesos, deterioro de imagen de la entidad ante el público, información inoportuna, procesos incumplidos.	
	Control de seguridad en los sistemas informáticos.	Perdida de información, retaso en los procesos, deterioro de imagen de la entidad ante el público, información inoportuna, procesos incumplidos, alteración de la operaciones administrativas	
	Identificación de riesgos en la seguridad de la información	Incumplimiento de procesos	
	Monitoreo constante en los sistemas de información y comunicación	Información errónea,, accesos no autorizados	

	Carecen de alternativas de salvaguardar la información ante la caída de los sistemas de información.	Información inoportuna fuera de fecha de proceso, respaldos inadecuados	
	Información no confiable	Demora en los procesos, perdidas de credibilidad de la imagen de la entidad ante el público,	
ADMINISTRATIVO	Contrato de servicio de vigilancia Anual	Aplicación de normas de cada empresa de seguridad al contratar	SEGURIDAD FISICA Y DEL ENTORNO, CONTROL DE ACCESO.
	Acceso no autorizados a las instalaciones	Falta de control del personal de vigilancia y aplicación de normas de seguridad internas del MTOP.	
	Registro de visitantes	Registran de manera Manual en un cuaderno	
	Verificación de los servidores si se encuentran en las instalaciones	No tienen teléfonos para comunicarse con el servidor a visitar para permitir el ingreso	
	Horario de visitas	No respetan horarios de oficina	
	Control de horario del personal	Registran de manera Manual en un cuaderno	
	Registro ingresos y salidas visitantes y personal	El guardia no siempre registra a todas las personas porque no está en su lugar de trabajo	
	Bitácoras de registros	El encargado de la Administración no solicita el informe di ario de vigilancia	
	Monitoreo cámaras de vigilancia	No pueden vigilar por medio de las cámaras de seguridad por falta de equipo de cómputo.	
	Carencia de control de seguridad en las noches	No hay un mecanismo de vigilancia de la parte exterior de las instalaciones.	
	Plan organizacional para control de visitas y servidores	Desorganización en proceso de vigilancia.	
BODEGA	Políticas de seguridad de la información de bodega	Perdida de bienes	GESTION DE ACTIVOS, SEGURIDAD FISICA Y DEL ENTORNO
	Plan estratégico de control de bienes	Perdida de información	

	Automatización de inventario de bienes.	Incumplimiento con solicitud de información	
TALENTO HUMANO	Políticas de contratación	Incumplimiento de tareas asignadas. Retraso en la entrega de trabajos	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS
	Cumplimiento de roles	Información no confiable. Tareas no satisfactorias.	
	Discreción de la información.	Manipulación de información por personas externas, antes de dar a conocer	
	Plan estratégico de Talento Humano	No se respeta los perfiles de los puestos.	
	Tiempo de contratación 2 años	Pérdida de tiempo en la culminación en los procesos de las tareas asignadas	
	Terminación de contrato en el MTOP	Perdida de información.	
TECNOLOGIA	Inadecuado desarrollo de software y adquisición de hardware	Inversión económica inadecuada. Suspensión de los sistemas de información. Inestabilidad en los procesos - fallas en la red.	GESTION DE ACTIVOS, SEGURIDAD FISICA Y DEL ENTORNO, CONTROL DE ACCESOS, ADQUISISCIÓN, DESARROLLO Y MATENIMIENTO DE SISTEMAS, GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.
	Mal uso de la información	Toma de decisiones no adecuadas.	
	Vulnerabilidad del sistema de información	Inversión económica inadecuada. Inestabilidad de los procesos. Filtro de información	
	Daños, deterioro o pérdida de los recursos tecnológicos	Equipos obsoletos, desperdicio de los recursos tecnológicos	
	Fallas en las redes de telecomunicaciones y sistema eléctrico	Perdida de información, retaso en los procesos, deterioro de imagen de la entidad ante el público, información inoportuna, procesos incumplidos.	
	Desconocimiento del Plan Estratégico	Desconocimiento.	
	Fracaso de eventos programados	Inversión económica inadecuada, incumplimiento con los técnicos	

	Accesos no autorizados a las instalaciones del área tecnológica	Daños, manipulación, robos en la infraestructura tecnológica	
	Desconocimiento de metodologías de respaldo de información	Desconocimiento.	
	desactualización de antivirus anti malware	Desactualización de antivirus	
	inadecuada adquisición y actualización de licencias	Inversión económica inadecuada,	
	Fallas en la Administración de Base de datos	Perdida de información, retaso en los procesos, deterioro de imagen de la entidad ante el público, información inoportuna, procesos incumplidos.	

Fuente: Elaboración propia.

Apéndice D

Valoraciones

Figura 5: Valoración de Activos

VALORACION DE ACTIVOS

Valoración de activos

Valor	Disponibilidad	Integridad	Confidencialidad
5	Este nivel abarca toda información, instalación o recurso cuya disponibilidad siempre debe garantizarse. Su pérdida es considerada como catastrófica para la Institución.	Este nivel abarca toda información, instalación o recurso en el cual la integridad es en extremo importante y debe garantizarse bajo cualquier circunstancia. Su pérdida es considerada como catastrófica.	Este nivel abarca toda información, instalación o recurso calificado como de uso confidencial. Solo puede ser utilizado con autorización explícita
4	Este nivel abarca toda información, instalación o recurso cuya disponibilidad puede estar detenida por algunas horas.	Este nivel abarca toda información, instalación o recurso en el cual la integridad es muy importante y debe garantizarse.	Este nivel abarca toda información, instalación o recurso calificado como de uso restringido. Solo puede ser utilizado por personal autorizado.
3	Este nivel abarca toda información, instalación o recurso cuya disponibilidad puede estar detenida por 24 horas máximo.	Este nivel abarca toda información, instalación o recurso en el cual la integridad es de importancia media y debe garantizarse.	Este nivel abarca toda información, instalación o recurso calificado como de uso semi-restringido. Solo puede ser utilizado por personal interno.
2	Este nivel abarca toda información, instalación o recurso cuya disponibilidad puede estar detenida por 48 horas máximo.	Este nivel abarca toda información, instalación o recurso en el cual la integridad no es muy importante pero debe garantizarse.	Este nivel abarca toda información, instalación o recurso calificado como de uso interno. Solo puede ser utilizado por personal interno o usuarios/clientes.
1	Este nivel abarca toda información, instalación o recurso cuya disponibilidad puede estar detenida por varios días sin causar consecuencias.	Este nivel abarca toda información, instalación o recurso en el cual la pérdida de integridad es insignificante.	Este nivel abarca toda información, instalación o recurso calificado como de uso público.

Fuente: Articulo Técnico SGSI, Jaime Michelena

Tabla: Valores degradación de Activo

DEGRADACION DEL ACTIVO

DESCRIPCIÓN	DEGRADACIÓN	VALOR
Baja	25	1
Media	50	2
Alta	75	3
Total	100	

Fuente: Articulo Técnico SGSI, Jaime Michelena

Tabla: Valores de Frecuencia de amenazas

VALORES REPRESENTATIVOS DE FRECUENCIA DE AMENAZAS EN ACTIVOS

VALOR	TASA	OCURRENCIA	TIEMPO
4	100	Muy frecuente	a diario
3	100	Frecuente	Mensualmente
2	100	Normal	una vez al año
1	1/10	Poco Frecuente	cada varios años

Fuente: Articulo Técnico SGSI, Jaime Michelena

Tabla: Valores de Frecuencia de amenazas

NIVELES DE VALORACIÓN DE RIESGOS

Nivel de factor de riesgo	Valor	Porcentaje
Bajo	1 a 32	1 a 25
Medio	33 a 63	26 a 50
Alto	64 a 94	51 a 75
Extremadamente alto	95 a 125	76 a 100

Fuente: Articulo Técnico SGSI, Jaime Michelena

Apéndice E

Encuesta Final

1. ¿Las políticas de seguridad determinadas en desarrollo del Plan de Seguridad de la Información, les permite a Ustedes como servidores público, deslindarse de responsabilidades como propietario de la información? Si……...NO……..

2. ¿Usted considera que la implementación de políticas de seguridad de la información le restringe al acceso de la información? ……...Si……**N**o.

3. ¿Las políticas de seguridad de la información permitirán una mejor administración de la información? Si……NO.

4. ¿El tener documentado las falencias que ocurren en los sistemas de información maximizara la credibilidad de la información? Si……..NO……

5. ¿EL plan de seguridad de la Información el momento de ser implementado se obtendrá información confiable, integra y disponible para la toma de decisiones de las autoridades? Si……..NO

Apéndice F

Registro Fotográfico

Figura: Archivos

Figura: Cableado de Red

Figura: Acceso a Edificio

Figura: Registro de Ingreso y Salida de visitantes

Figura: Incidentes Sistema QUIPUX

Estimados:

Funcionarios, Servidores Públicos y Trabajadores del Ministerio de Transporte y Obras Públicas, Ponemos en conocimiento que el sistema Quipux, no es una herramienta de nuestra institución, pertenece a la Subsecretaría de Gobierno Electrónico, Secretaría Nacional de la Administración Pública, el cual a través de correo electrónico, informa:

Mediante el presente, se notifica un incidente en el sistema de Gestión Documental Quipux:

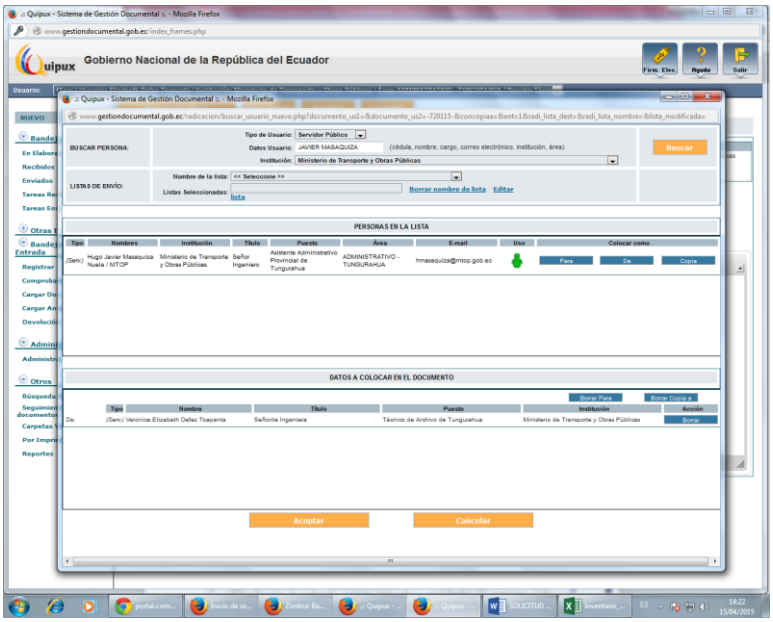
Fecha Inicio: 17 de abril de 2015
Hora Inicio: 11:45
Fecha Fin: 17 de abril de 2015
Hora Fin Estimada: 14:00
Duración Estimada: dos horas quince minutos

Comportamiento Actual: No se pueden visualizar algunos pdf.

Por favor su ayuda comunicando este particular a los usuarios del sistema.

Fuente: Correo Zimbra

Figura: Ex Servidor habilitado en el Sistema.



Fuente: Sistema Quipux

Figura: Correcciones SITOP

De: "MOYA MEDINA DILON GERMAN" <dmoya@mtop.gob.ec>
Para: "ORTIZ DURAN DEYSI JEANNETTE" <djortiz@mtop.gob.ec>
Enviados: Viernes, 17 de Abril 2015 10:57:45
Asunto: Fwd: CORRECCIONES EN EL SISTEMA SITOP

Estimada Deysi

Por favor que el Técnico encargado (Ing. Reyes), corriga en forma urgente lo solicitado

De: "CARDENAS ALVARRACIN MARCELA EDITH" <mcardenas@mtop.gob.ec>
Para: "MOYA MEDINA DILON GERMAN" <dmoya@mtop.gob.ec>
CC: "ORTIZ DURAN DEYSI JEANNETTE" <djortiz@mtop.gob.ec>, "ONA CHANGOLUISA NORMA PATRICIA" <nona@mtop.gob.ec>, "DAVILA CADENA CHRISTIAN ROBERTO" <cdavila@mtop.gob.ec>, "GUALPA CASTILLO NANCY JACQUELINE" <jgualpa@mtop.gob.ec>
Enviados: Viernes, 17 de Abril 2015 10:50:27
Asunto: CORRECCIONES EN EL SISTEMA SITOP

Estimado Ing:

Solicito de manera urgente su ayuda para que pueda ser corregido en el sistema SITOP los siguientes contratos:

17/04/2015

https://correo.mtop.gob.ec/h/printmessage?id=5953&tz=America/Bo

ID	CONTRATO	A REVISAR
3400	CONSULTORIA DE LA CARRETAR AMBATO-PASA-CORAZÓN	Monto contractual
9819 -RIOBAMBA	CONTRATO PARA LA AMPLIACIÓN DEL TRAMO AMBATO	Falta situacion actual

Por su gentil colaboración, anticipo mis agradecimientos.

Saludos cordiales;

--
Ing. Marcela Cárdenas A.
Asistente de Planificación
Dirección de Planificación Intersectorial de la Movilidad
Telf.: + (593-2) 3974 600 **Ext. 20060**
mcardenas@mtop.gob.ec
www.obraspublicas.gob.ec
Quito - Ecuador.

Fuente: Correo Zimbra

Referencias

[1] AVELLANEDA, J., Sistemas de Gestión Seguridad de la Información, 2014.

[2] BUENAÑO, Jose., Granja, M., Planeación y Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001-27002.2

[3] CESCALM., Recomendaciones para el Desarrollo de un Plan de Seguridad de la Información, 2011.

[4] INTECO., Conceptos Básicos sobre la Seguridad de la Información, 2010.

[5] INTECO, *SGSI* - 05 Implantación de un SGSI, 2010.

[6] INTECO, Guía Gestión de Fuga de Información, 2012.

[7] ISO 27000., Sistema de Gestión de la Seguridad de la Información, 2014.

[8] Metodología para la Gestión de la Seguridad Tecnología (Proyecto), 2013.

[9] PEÑAHERRERA, C., Acuerdo 166, SNAP, 2013.

[10] PALLAS G, Metodología de Implantación de un SGSI en un grupo empresarial jerárquico, Tesis, 2009.

[11] TECHNOPAT., Sistema de gestión de la seguridad de la información, 2014.

[12] VILLALBA, M., ISO 27000, 2013.

[13] MICHELENA, J., Díaz Paola, Articulo Técnico SGSI, 2014.

[14] INFAI, Guía para implementar un Sistema de Gestión de Seguridad, 2013

[15] BALDECHI R., Implementación efectiva de un SGSI ISO 27001, 2014

[16] ORMELLA, C., Normas ISO De Seguridad de la Información, 2014

[17] ISO 27000, Controles ISO 27002, 2013.

[18] LÓPEZ, E., Seguridad de la Información, 2013.

Resumen Final

Desarrollo De Un Plan De Seguridad De La Información Basado En Las Normas INEN ISO/IEC 27000 Para El Ministerio De Transporte Y Obras Públicas

Verónica Elizabeth Defaz Toapanta.

109 páginas

Proyecto dirigido por: Darío Robayo Jácome, Mg.

En el presente proyecto diseñado para el Ministerio de Transporte y Obras Públicas, se establece posibles soluciones de seguridad de la información en base a los Estándares de las Normas INEN ISO, lo que actualmente se está implementado conforme al Acuerdo 166.

El primer Capítulo se plantean los lineamentos iniciales del proyecto, presentación, detección del problema, y detalles del proyecto del porque la factibilidad del desarrollo de políticas de seguridad de la información

El Segundo Capítulo se plantea la propuesta de trabajo, dando a conocer información básica, metas, objetivos y delimitación del mismo.

En el tercer Capítulo se hace hincapié a conceptos de términos que serán utilizados en el desarrollo del presente proyecto permitiendo tener claro de lo que se va aplicar y lo que abarcaría.

El Cuarto Capítulo se detalla la metodología a utilizar y los estándares aplicarse, realizando un análisis actual de los procesos administrativos de la institución que han sido identificados conforme a las observaciones en el sitio y entrevistas planteadas, a su vez se detalla el análisis de riesgos identificando los activos, responsabilidades, vulnerabilidades.

Capítulo 5 se detalla los resultados es decir se han definido las políticas de seguridad conforme a los 11 dominios del estándar seleccionado ISO 27002, identificando los controles adecuados para minimizar los incidentes identificados, designando responsabilidades para posteriormente con órdenes de la Máxima autoridad ser implementados y cumplir con toda la metodología PDCA.

Finalmente el Capítulo 6 de conclusiones y recomendaciones, en el presente proyecto no se detalla costo de implementación porque para el mismo se debe realizar un análisis exhaustivo de las herramientas a utilizar para cumplir con los controles de las políticas planteadas, este análisis se lo realiza en el momento de ejecutar el PSI, porque ahí se determinaran que tipo de hardware, software y personal serán necesarios.