ESTUDIO Y DIAGNOSTICO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL INSTITUTO NACIONAL DE VIAS INVIAS PLANTA CENTRAL

MARIBEL CRUZ ARGUELLO

UNAD

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ

ESTUDIO Y DIAGNOSTICO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL INSTITUTO NACIONAL DE VIAS INVIAS PLANTA CENTRAL

MARIBEL CRUZ ARGUELLO

Proyecto de Grado para optar al Título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Ingeniera
YINA ALEXANDRA GONZÁLEZ SANABRIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA.
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ
2019

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

_____

Firma Del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá, marzo 26 de 2019

DEDICATORIA

Este trabajo de Investigación lo dedico en honor en nombre de mis Hijos Andrés Felipe Herrera Cruz Y Sergio Alejandro Herrera Cruz. A mi esposo Carlos Alfonso Herrera, por su énfasis en superar las barreras. Y en especial a mis padres quienes siempre me alentaron, forjaron y fortalecieron en un mejor futuro para mí y mi generación de hermanos y que igualmente dieron fe en que este sería la vía para el logro de nuestros sueños y esperanzas, “nuestra educación”.

Como también a todos mis compañeros de trabajo y de grupos colaborativos de los cuales forme parte durante mi formación academia, importantes en el desarrollo y cumplimiento de mis metas propuestas y que me han acompañado igualmente con su apoyo en todos estos proyectos.

Y grandemente a Dios por la vida y la esperanza de un mundo mejor.

AGRADECIMIENTOS

Este trabajo de Investigación, optado como proyecto de grado se ha venido desarrollando como parámetro inicial a un esfuerzo de quienes poseemos la responsabilidad y la obligación como Especialistas en Seguridad de la información, en formación por la Universidad Nacional Abierta y a Distancia UNAD, y que hemos decidido culminar.

A todo el equipo de docentes que nos acompaña, con su entrega y entereza en nuestra formación y en especial a la Ingeniera Doc. Yina Alexandra González Sanabria, quien nos asiente y acompaña durante todo el estudio de investigación aplicada, que se ha venido elaborando a conciencia.

Como también a nuestros docentes y a nuestra alma mater universitaria UNAD, por el apoyo, formación y calidad en la educación, la que nos invita con la altivez acostumbrada local, regional y nacional, a sumar grandes retos a nuestra vida profesional.

CONTENIDO

LISTA DE TABLAS

LISTA DE IMÁGENES

LISTA DE ANEXOS

GLOSARIO

- **Dato:** se llama dato a lo que en informática se llama atributo o variable. representan un fragmento de una cantidad, medida, descripción o palabra.
- **Estándar:** Hace referencia a una norma o especificación general de elemento fundamental, en el momento de hablar de gestión de datos e información.
- **Control:** herramienta o proceso de verificar el desempeño de un elemento dentro de un proceso administrativo, como la autenticación, autorización de acceso y auditoría.
- **Gestión:** conjunto de acciones encaminadas a la administración de un proceso, dirigido a alcanzar los objetivos propuestos de la entidad.
- **Guía:** Es un principio o procedimiento que encauza información referente a un asunto específico, hacia un objetivo.
- **Información:** procesos estructurados, que construyen un mensaje orientado a resolver una problemática, mediante códigos o modelos de desarrollo.
- **Mapa de procesos:** Representación gráfica aplicada, para demostrar visualmente todos los pasos en un proceso dado, reflejando de forma detallada y profunda el funcionamiento de las tareas en la entidad.
- **Política de calidad:** Acción que se integra al manual de función de la entidad, con el compromiso de la dirección, como mejora continúa.
- **Procedimiento:** Acción o método que se ejecuta, basado en una actividad o proceso especifico.

- **Responsabilidad:** Resultados y obligaciones, que recaen sobre el mismo, Comprimiendo y garantizando los compromisos adquiridos que se generan en una tarea.
- **Rol:** Tarea que recae sobre el particular del rol, encargado de las funciones de seguridad, como el proveedor del servicio.

- **Protección de la Información**. Garantía de integridad, medio y disponibilidad de la información.

- **Sistema de información**. Componentes estratégicos de la información "Activos, Tecnología y Datos" en el administración de la información.

- **Tramite:** conjunto de pasos y acciones que identifican una solicitud de forma sucesiva para dar solución a un proceso.

- **Tratamiento:** Forma o medio utilizado para llegar a la esencia de un proceso elaborado o resultante de una operación técnica de carácter automatizado o no.

- **Vulnerabilidad.** Falla de control o agotamiento de un activo que presenta o ha presentado acceso directo y se hace sensible a un intruso informático "Virus".

1. INTRODUCCIÓN

Dentro de los 12 procedimientos que paso a paso se han elaborado y adaptado para el funcionamiento y manejo de la información al interior del Instituto Nacional de Vías INVIAS, son el resultado de una ardua investigación y aplicación de las normas que sobre políticas de seguridad de la información han sido propuestas por cada uno de los entes normativos y jurídicos del estado colombiano, dando cumplimiento al logro de los objetivos misionales de la entidad y como herramienta básica en la toma de decisiones .

El diagnóstico inicial, guiara a la entidad en la búsqueda y Gestión en el manejo adecuado del riesgo informático, la inversión en tecnologías de la información y la comunicación, bajo la normatividad actualizada existente y de la mano con las plataformas de información conocidas como:

- **Vive Digital**: Esta plataforma tecnológica busca estabilizar al país en los próximos años, mediante la masificación del uso del internet y del ecosistema Digital, nacional.

- **Convertic:** Proyecto tecnológico del Ministerio de Tecnologías de la Información y las Comunicaciones, y que a través de su Plan Vive Digital lanza Convertic, brindando la descarga gratuita y a nivel nacional, de software accesible, aportando la inclusión social como estrategia de conectividad tecnológica, en busca del beneficio de la población vulnerable.

- **Centro de Relevo**: Herramienta de apropiación Tic, con apoyo de la Federación Nacional de sordos de Colombia para beneficio y soporte de la población con discapacidad auditiva de todo el país. Proyecto que busca la optimización de la gestión pública a través del uso estratégico de la Tecnología.

- **Gobierno en Línea**: Igualmente Toda la plataforma Tecnológica en conjunto, del INVIAS, favorece el trabajo colaborativo, la participación ciudadana, la publicidad y transparencia de la gestión Institucional, permitiendo establecer la comunicación en línea trazada por el gobierno nacional, a través de la Ley de Transparencia, el Plan Anticorrupción y el componente de Seguridad y Privacidad de la Información, de las entidades Públicas.

2. SITUACIÓN ACTUAL

Los servicios tecnológicos, información y de Comunicación en el Instituto Nacional de Vías INVIAS, se ofrecen gracias a la infraestructura técnica, tecnológica y de seguridad de la información, con la que se cuenta desde el año 1.994 y de sus nuevas adquisiciones.

A su vez el Estado Colombiano diseñó la estrategia Gobierno En Línea – GEL, la cual establece los lineamientos de la gestión de TI en el sector Gobierno, recogiendo estándares mundiales y mejores prácticas de gobierno electrónico y de buen uso de la tecnología como herramienta de publicidad y transparencia.

Para lograr lo anteriormente establecido, se plantea como herramienta transversal el Marco de Referencia de Arquitectura Empresarial, que orienta sobre mejores prácticas, guías y estándares en el uso adecuado de la tecnología como soporte de procesos y servicios, orientados al cumplimiento de la norma y misión del Instituto Nacional de Vías INVIAS.

En cumplimiento de la Estrategia GEL y acorde con el desarrollo Tecnológico, en INVIAS se ofrecen los servicios tecnológicos, agrupados según el beneficio general que se reciben y perciben los usuarios, para que sean de mejor entendimiento, así:

- Servicios de ofimática
- Servicios de conectividad/comunicaciones
- Sistemas de información
- Soporte técnico
- Servicios seguridad de la información.

Recursos tecnológicos que INVIAS pone a disposición de trabajadores, Contratistas y ciudadanos, para proveer y optimizar el trabajo y la consulta de sus aplicaciones.

3. CONSIDERACIONES PREVIAS

3.1 Definición

El instituto Nacional de Vías, debe optimizar los conceptos y lineamientos para establecer la actualización de las políticas de Seguridad de la Información, mediante su estudio y diagnostico general.

El Instituto Nacional de Vías INVIAS, tiene en la actualidad un Manual de Políticas y Normas de Seguridad para la información y su acceso, adoptado mediante Resolución No. 1364 de 2016. Sin embargo y teniendo en cuenta, el vertiginoso desarrollo y evolución que tienen las herramientas tecnológicas, con los consabidos riesgos que ello representa, es necesario hacer una revisión y diagnóstico de las políticas actuales, con el fin de identificar las mejoras que se puedan aplicar y proponer la actualización correspondiente.

Ante las deficiencias en cuestión sobre “Seguridad de la Información” que se trazan en este documento escrito, concibe necesariamente realizar los ajustes y modificaciones a dicho sistema, es por ello de gran importancia que la información este bien protegida de ataques informáticos y de las posibles pérdidas de la misma.

Para dar inicio al proyecto primero se identificaran los activos de información, las Amenazas y Debilidades, para luego dar paso a aquellas vulnerabilidades a las que se pueden ver expuestos dichos activos, seguido de un análisis a las políticas y normas existentes que los protejan y minimicen el riesgo de ocurrencia. Seguido de la formación de la propuesta de mejoras a las políticas existentes, para finalmente elaborar un documento final con las mejoras establecidas.

La metodología será de tipo investigación aplicada con trabajo de campo a través de la observación y el análisis de la documentación existentes y de las entrevistas a funcionarios que posean información estratégica, para el proyecto.

Como resultado final se presentara un escrito como documento dictamen y las sugerencias necesarias para la adaptación, actualización y/o nuevas directrices y políticas, en materia de “Seguridad” para la “Información”.

3.2 Formulación

Actualmente el Instituto Nacional de Vías INVIAS, peligrosamente presenta un aplazamiento en la actualización de políticas y normas de protección de sus diferentes sistemas de información.

Por ello es de gran importancia plantearnos ¿cuáles son los ajustes que se requieren para implementar unas políticas de seguridad actuales, que permitan proteger adecuadamente todo tipo de información existente en el instituto Nacional de Vías?

Se cuenta con un manual sobre las “Políticas de Seguridad de la Información” revisadas y aprobadas en el año 2014, que deben ser actualizadas, partiendo de las “Políticas de Seguridad y Privacidad” sugeridas por el “Modelo de Seguridad y Privacidad de Gobierno en Línea (GEL) en su versión anterior.

Un análisis preliminar nos permite evidenciar que no se tienen en cuenta los parámetros actuales de los sistema de información que se han venido involucrando a raíz de los cambios de plataformas informáticas, donde se deja al descubierto “cuartos oscuros”, “Vulnerabilidades, Riesgos y/o Amenazas, a las que

singularmente se expone la información que está vigente en cada uno de los procesos internos, de la entidad[1].

Así también se puede observar, que aún no están estandarizadas estas políticas de seguridad, por lo tanto no tienen normalizados los controles que llevan a mitigar de forma directa una amenaza y por lo tanto la información está expuesta al ciberdelito, ni a los datos que se comprometen en su integridad, confidencialidad y disponibilidad.

En la actualidad hay procedimientos creados por simple iniciativa y experiencia del jefe del área de informática; es el caso por ejemplo del servidor que tiene que ser apagado para permitir la migración de la información a la nueva plataforma informática, generando tardíos accesos a la red y caídas inesperadas de la misma. Aunque coexiste la política de uso de "claves de usuarios", el servidor continuamente se ve expuesto a cambios de "Claves de acceso" a juicio único y sin una bitácora definida.

La Entidad tiene algunas dificultadas e inconvenientes dentro del manejo de la información pues se debe extender al territorio nacional, por sus unidades ejecutoras territoriales y no se ha creado conciencia sobre el valor que es el de asegurar la información histórica creando entonces la necesidad de adaptar y ampliar de manera ágil la actualización de estas "Políticas" que pauten las buenas prácticas en cada uno de los procesos y recursos, relacionados con la "Información".

[1]Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca- John Jairo Perafán Ruiz Mildred Caicedo Cuchimba.
http://repository.unad.edu.co/bitstream/10596/2655/3/76327474.pdf

Se hace necesario entonces efectuar un nuevo análisis del SGSI dentro del INVIAS, incluyendo los activos que están relacionados con estos procesos, identificando y eliminando los riesgos que se presentan y que afectan la "Seguridad de la Información", con el fin de actualizar las "Políticas de Seguridad de la Información" dentro del "Sistema de Gestión de Seguridad de la Información". De no actualizar estas políticas se puede ver interrumpido el normal funcionamiento de los servicios informáticos y perder la información a nivel territorial.

4. DELIMITACIÓN

Espacial: Instituto Nacional De vías-INVIAS. Sede Central Bogotá
Demográfica: Estudiante, Funcionarios, Directivos y Contratistas.

Temporal: 01 de mayo de 2018 a Julio de 2018
Temática: Análisis de Riesgos, Amenazas y "Políticas de Seguridad de la Información", programación y control.

Se tiene como punto de partida a la entidad, centralizada en la ciudad de Bogotá, sede central, ubicada en el barrio Centro Administrativo Nacional CAN, para realizar el estudio de Investigación, por ser Líder Organizacional, Administrativo y Financiero en todo el territorio nacional, la cual permite el desarrollo de esta clase de trabajo investigativo.

Contraste a las demás entidades territoriales y que dependen de la sede central, que también son dependencias abiertas para cualquier investigación y desarrollo por su servicio cotidiano, pero distante al sujeto investigativo.

Es indiscutible que por razones de pertinencia y cercanía se hace más fructuoso el estudio de un escenario donde desempeñamos nuestras funciones y que podamos obtener toda la información, de la mano de los responsables de la misma.

Igualmente, la escogencia del periodo comprendido por los meses de mayo a julio de 2018 nos da campo y cumple lo que se requiere en una metodología de investigación aplicada, la forma de establecer los impactos que se genera de la información de origen o de creación de la misma.

Se realizan también intervenciones de acuerdo a las políticas establecidas de la entidad acorde al nivel de trabajo de la misma y bajo otras investigaciones que se han realizado con antelación a la que se desarrolla.

5. ANTECEDENTES DE LA INVESTIGACIÓN

Formal al tema propuesto "Políticas de Seguridad de la Información", distintas entidades del Estado Colombiano, Empresas en Colombia y del exterior, implementan estas "Políticas de Seguridad", en "Manuales", como guías que siempre deben estar disponibles y documentadas.

El punto de partida es:

- **La norma ISO/IEC 27001:2013** *Norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. Es la principal norma a nivel mundial para la seguridad de la información*[2]*.*

- **Universidad de CONCEPCIÓN, CHILE. Modelo Para "Seguridad de la Información" en TIC, autor Jorge Burgos Salazar1 y Pedro G. Campos.**

Este trabajo ejemplariza la importancia y la urgencia que representa la seguridad de la información hoy en día y se discuten brevemente los diversos aspectos involucrados en la formulación del modelo.

Se presentan las normas, estándares y leyes más relevantes relacionadas con el tema, y se discuten brevemente los diversos aspectos involucrados en la formulación del modelo y facilitar la obtención de un adecuado nivel de control de riesgos en Tecnologías de Información y Comunicación (TIC), que permita entre otros evitar y/o disminuir las fallas en los sistemas, redes, Internet y todo el patrimonio informático (hardware, software y datos) de ataques o desastres, antes que éstos ocurran"[3]*.*

---

[2]ISO 27000.es http://www.iso27000.es/glosario.html

[3] Modelo Para Seguridad de la Información en TIC. Jorge Burgos Salazar1, Pedro G. Campos1,Universidad del Bío-Bío, Avenida Collao 1202, Casilla 5-C P:4081112,Concepción, Chile http://ceur-ws.org/Vol-488/paper13.pdf.

- **Ministerio De Defensa Sevilla, España**. ***Política De Seguridad De La Información Del Ministerio De Defensa***. Néstor Ganuza Artiles Comandante Ejército de Tierra Área de Seguridad Inspección General CIS Secretaría de Estado de Defensa Ministerio de Defensa.

Aquí la implementación de La Política de Seguridad del Ministerio de Defensa es el conjunto de normas y procedimientos que proporcionan dirección y soporte para la gestión de la seguridad de la información dentro del Ministerio de Defensa. Tecnimap 2006. Sevilla, donde "*La elaboración y aprobación de la Política de Seguridad de la Información del Departamento es el proyecto más significativo del Área de Seguridad de la Inspección General de Sistemas de Información y Comunicaciones del Ministerio de Defensa (en adelante IGECIS)*[4]*.*

- **Policía Nacional de Colombia**, bajo la Resolución Número 08310 de 28 Diciembre de 2016, expide el "***Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional***".

Da a conocer "*Que a través de la Resolución 03049 del 24 de agosto de 2012, se adoptó el Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional. Y que la Policía Nacional mediante la implementación del Sistema de Gestión de Seguridad de la Información, busca proteger los activos de la información como insumo fundamental para el cumplimiento de la misión y asegurar la supervivencia de la Institución, protegiéndola a través de la aplicación efectiva de las mejores prácticas y controles y garantizando la gobernabilidad del país"*[5]

[4] Norma, fundamental para la construcción de la Seguridad de la Información. file:///C:/Users/Familia%20Herrera/Downloads/politica_de_seguridad_de_la_informacion.pdf

[5] la implementación del Sistema de Gestión de Seguridad de la Información http://www.policia.edu.co/sgsi/resolucion%2008310%20de%2028122016-%20manual%20sgsi.pdf

- ***Presidencia de la Republica***, documento ***"Manual de Políticas de Seguridad de la Información, como proceso asociado a las tecnologías de información y Comunicación".***

Trabajo que muestra "*La importancia y sensibilidad de la información, el DAPRE integra el sistema de la información SGSI, dentro del sistema de Gestión de la Presidencia de la Republica SIGEPRE de tal forma que permite generar la mejora continua del sistema de seguridad, basados en la gestión de riesgos y continuidad de la entidad*"[6]

5.1 Revisión Bibliográfica

Una revisión bibliográfica relacionada con los temas tratados aquí, ha realizado grandes aportes conceptuales y relacionados en la investigación y los procedimientos establecidos como elementos básicos de la ***investigación aplicada,*** en la situación actual.

- Norma NTCGP 1000 y el estándar internacional ISO 9001[7].
- Guía Metodológica de Pruebas de Efectividad, Instrumento de Evaluación MSPI. 18 de noviembre de 2017. Ministerio de las Tics.
- Controles de "Seguridad y Privacidad de la Información". Bogotá 18 de noviembre de 2017. Ministerio de las Tics. Y de Las Comunicaciones. políticas de seguridad para las entidades del Estado, que de forma innovadora encuentren las mejores prácticas y experiencias de otros países y las adapten para que las Entidades Colombianas cuenten con los mejores estándares en esta materia".
- Manual de "Políticas de Seguridad de la Información". Manual de Calidad Y Gestión Integral Instituto Nacional de Vías, INVIAS.

[6] Manual-Políticas-Seguridad-Información. http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/M-TI-01-Manual-Politicas-Seguridad-Informacion.pdf
[7] Qué es la NTC GP 1000 y para qué sirve en la Administración Pública? https://gestion.pensemos.com/que-es-la-ntc-gp-1000-y-para-que-sirve-en-la-administracion-publica

6. JUSTIFICACIÓN.

La implementación de estos ajustes al Manual de Políticas y Normas de Seguridad de la Información, se muestran como una necesidad vital para el INVIAS, ya que de su socialización y apropiación, depende el correcto funcionamiento de todas sus dependencias, tanto de sus diferentes proyectos viales, como de su normal funcionamiento financiero, presupuestal y hasta de manejo de personal.

Este documento a presentar, mostrará de forma actualizada, el (SGSI) o Sistema de Gestión de Seguridad de la Información, que asentirá mantener una guía de negocio sólida, como valor agregado y empoderamiento a nivel Regional.

Pretende presentar un programa estratégico organizacional e incorporar las mejoras en los procesos relacionados con las gestión Tecnológica en la entidad, que se desarrolla en tres fases, la primera en cuanto a las "Políticas de Seguridad de la entidad (INVIAS), la segunda está integrada por las "Normas de Seguridad " en relación directa a la ejecución y soporte de las "Políticas de Seguridad de la Información" y una tercera que involucra los diferentes niveles de seguridad, teniendo en cuenta qué activo informático de la entidad se va a proteger, de que protegerlo, como protegerlo y por qué protegerlo; bajo el esquema normativo de seguridad GEL/ISO 27000.

El desarrollo de este proyecto permitirá primero que la entidad cuente con normas y Políticas de seguridad actualizadas, que la información que se presente al público sea veraz y a la ves este protegida, lo que redundará en mayor transparencia, conocimiento y valoración de la labor adelantada por la entidad.

Al mismo tiempo el presente proyecto permitirá aplicar los conocimientos impartidos durante el programa académico de una manera real a un problema real y potencializando las habilidades y capacidades adquiridas; formulando soluciones a problemas del medio informático y de allí la gran trascendencia, pertinencia y utilidad del proyecto.

7. OBJETIVOS

7.1. OBJETIVO GENERAL

Analizar el Manual de “Políticas y Normas de Seguridad de la Información” del Instituto Nacional de Vías INVIAS, para plantear su actualización de acuerdo con el modelo MSPI y reglamentado por el “Modelo de Seguridad y Privacidad” de Gobierno en Línea (GEL) y de los estándares actuales.

7.2. OBJETIVOS ESPECÍFICOS

- Identificar el activo informático que se va a proteger bajo el esquema normativo de seguridad GEL/ISO 27001:2013 y las áreas susceptibles de ataques o con problemas de seguridad dentro del INVIAS.

- Identificar las amenazas y debilidades del actual sistema de manejo y protección de la información. Metodología Magerit, actualizada en versión 3. Anexo Final.

- Diagnosticar las “Políticas de Seguridad”, privacidad y manejo de la información, existentes con las ajustadas a los estándares internacionales actuales.

- Elaborar Un documento final que incluya las actualizaciones, recomendaciones y formulaciones sobre “Políticas de Seguridad de la Información”, de tal manera que puedan ser aprobada y adaptadas por el Instituto Nacional de Vías, INVIAS. Anexo Final.

8. MARCO REFERENCIAL.

Para el componente referencial y conceptual y desarrollo de este documento, es de vital importancia la "Teoría General de Sistemas", esta teoría nos aporta la identificación de las diferentes características, parámetros y estructuras activas de los diferentes actores activos y visuales se producen a través de la toma de decisiones.

Por otro lado el elemento llamado " La Quinta Disciplina que se entiende como aquella capacidad que se tiene para cambiar la forma de hacer las cosas, siempre en busca del aprendizaje de nuevos cuestionamientos y que lo que hoy se hace bien, puede hacerse mucho mejor, aunque no de la forma que siempre se ha visto hacer.

En otras palabras extendiendo el argot de "organización inteligente" a una organización que debe adquirir nuevas habilidades que le permitan adecuarse a los cambios y a la Construcción de una visión compartida[8]

Siendo de vital importancia que una organización alcance el éxito si se ha propuesto la misión, las metas y los valores, compartidos dentro de la estructura empresarial, con el objetivo de llevar a cabo un trabajo importante y común.

8.1. MARCO CONTEXTUAL

El instituto Nacional de Vías INVIAS, es una entidad del sector central con personería y presupuesto propio, encargada de desarrollar las políticas de infraestructura vial, fluvial, ferroviaria y portuaria a nivel nacional.

[8] La Quinta Disciplina El arte y la práctica de las organizaciones que aprenden. Peter Senge. . Ed. Granica, 1994. http://www.jmonzo.net/blogeps/laquintadisciplina.pdf

Actualmente la sede central se encuentra en la ciudad de Bogotá y posee veintiséis (26) sedes regionales distribuidas a lo largo del país, su planta de personal es de alrededor de 700 personas en la planta central y 800 a nivel regional.

- **Organigrama** :

Figura 1.

Fuente: Instituto Nacional de Vías INVIAS[9]

Lo que deja a nivel central, estratégicamente ubicada para el estudio de investigación realizado, por su reconocido liderazgo en temas Organizacionales, Administrativos y Financieros.

[9] Instituto Nacional de vías INVIAS.
https://www.invias.gov.co/index.php/informacion-institucional/organigrama2018

Y se deja abierta, también la posibilidad para cualquier investigación y desarrollo por su quehacer cotidiano, a las entidades territoriales de la Organización estatal.

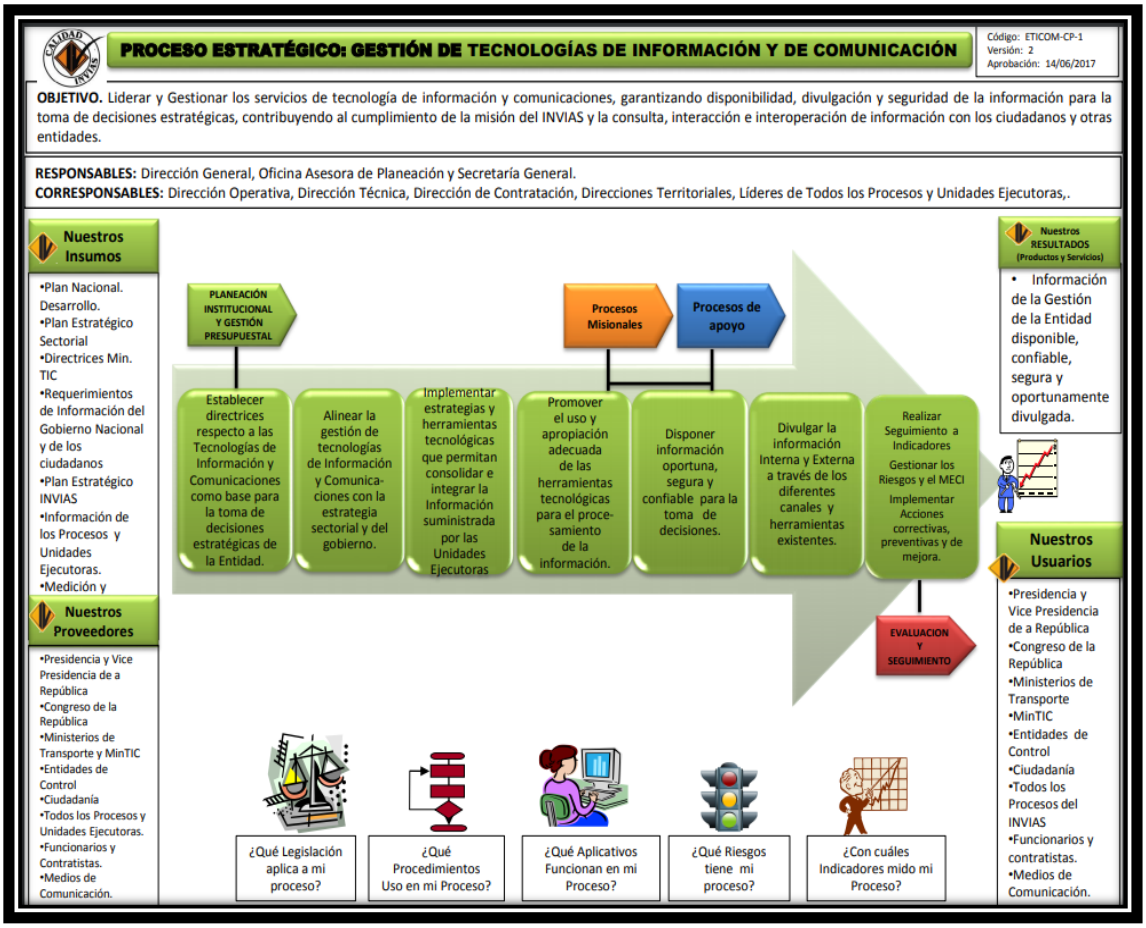
Es indudable que por razones también de permanencia, es más productivo realizar el análisis bajo un escenario donde se diariamente se realizan nuestras funciones como servidores públicos y que podamos obtener toda la información, de la mano de los responsables de la misma. Por lo que de manera general, la escogencia en Planta Central (Oficina Asesora de Planeación- Grupo de Gestión de Tecnología de Información y Comunicaciones), obedece entonces a la delimitación y desarrollo del trabajo, bajo una metodología de Investigación Aplicada, como la forma de establecer los impactos, con la información de origen o de creación de la misma.

Se realizan también intervenciones de acuerdo a las políticas establecidas de la entidad acorde al nivel de trabajo de la misma y bajo otras investigaciones que se han realizado con antelación a la que se desarrolla.

El manejo de los sistemas de información están a cargo de la unidad de Informática, que se encarga de determinar las “Políticas de Seguridad” y del manejo que todos los funcionarios deben seguir, bajo las directrices y prohibiciones en la administración de la información, que a este nivel se deben adoptar, dando manejo a las nuevas políticas de seguridad y guía de la información que se pretende formular.

- Gestión de Tecnologías de Información y de Comunicación

Figura 2. Proceso estratégico "Gestión de Tecnologías de Información y de Comunicación



Fuente: Instituto Nacional de Vías - INVIAS

Como parte de la implementación del documento final que incluya las actualizaciones, recomendaciones y formulaciones sobre políticas de Seguridad de la Información y la Política de Gestión y desempeño "Implementación de la Política de Fortalecimiento organizacional y simplificación de procesos", se aclaran dudas

sobre la mejor y más eficiente forma de ejecutar las operaciones de la entidad, Instituto Nacional de Vías-INVIAS.

Posteriormente se socializa la plantilla para documentar las caracterizaciones de proceso, donde de forma participativa se analizaron los avances en la actualización de los procesos.

Figura 3. Contextualización Modelo de Operación- Instituto Nacional de Vías INVIAS

Fuente. Instituto Nacional de Vías. INVIAS

8.2. MARCO TEÓRICO

8.2.1. La Quinta Disciplina. “Las organizaciones que utilizan prácticas colectivas de aprendizaje – como centro de competencia - están bien preparadas para prosperar en el futuro, porque serán capaces de desarrollar cualquier habilidad que se requiera para triunfar. En otras palabras, la capacidad de ganancia futura de cualquier organización está directa y proporcionalmente relacionada con su habilidad y capacidad para aprender cosas nuevas”. **Peter M. Senge. Ed. Granica, 1994.** [10]

8.2.2. Teoría General de Sistemas: La teoría de sistemas (TS) es un ramo específico de la teoría general de sistemas (TGS).

“Básicamente son los sistemas que existen dentro de sistemas abiertos y las funciones dependen de su estructura. Aquí cada sistema realiza tareas con la finalidad de cumplir con los objetivos planteados en representación de una dependencia superior, a la cual pertenece, y presenta beneficiados por las funciones de un determinado sistema”[11].

8.2.3 Gerencia Estratégica Esta herramienta está diseñada para administrar y ordenar los cambios, que definen los objetivos de la organización y se establecen estrategias para lograrlos. El reconocimiento y la participación basada en el liderazgo de los ejecutivos de la entidad para tomar las decisiones que correspondan a las demandas del ambiente inmediato y futuro.

“ Fundamentalmente basado en la identificación de amenazas y oportunidades externas de una entidad, al igual que las debilidades y fortalezas internas, la fijación de objetivos, el desarrollo de estrategias

[10] La Quinta Disciplina El arte y la práctica de las organizaciones que aprenden. Peter Senge. Ed. Granica, 1994. http://www.jmonzo.net/blogeps/laquintadisciplina.pdf

[11] Introducción a la Teoría General de Sistemas. Jo Hansen Bertoglio, O. Ed. Santa Fe. 2008. La teoría de sistemas (TS) es un ramo específico de la teoría general de sistemas (TGS)

alternativas, el análisis de dichas alternativas y la decisión de cuales escoger. Según Fred. R David Gerencia Estratégica es un proceso mediante el cual se formulan, ejecutan y evalúan las acciones que permitirán que una organización logre los objetivos"[12].

El Instituto Nacional de vías INVIAS, plantea dentro del plan estratégico institucional para el periodo 2015-2018, la visión "por una infraestructura vial nacional competitiva, que genere conectividad regional para un nuevo país".

"Y de esta forma El Gobierno Nacional a través de la ley 1753 del 9 de junio de 2015 expidió el Plan Nacional de Desarrollo "Todos por un Nuevo País" con el cual se establecen los lineamientos, objetivos y estrategias para el cuatrienio 2014-2018. Dicho Plan Nacional de Desarrollo se centra en los pilares de Paz, Equidad y Educación".

"Las directrices que emana el Plan Nacional de Desarrollo son producto de la socialización y participación ciudadana en las diferentes regiones del país y contiene los retos del Gobierno Nacional para la construcción de un Nuevo País: equitativo, educado y en Paz. En este sentido, el Ministerio de Transporte en coordinación con las entidades adscritas al sector Transporte formularon el Plan Estratégico Sectorial que recoge los lineamientos del Plan Nacional de Desarrollo y fija los retos del sector para el presente período de gobierno".

"Y Es así como El Instituto Nacional de Vías –Invías- comprometido con la Paz y la Equidad formula el presente Plan Estratégico Institucional que incluye los lineamientos del Gobierno Nacional, la priorización del Ministerio de Transporte, los objetivos y metas institucionales del cuatrienio, con lo cual busca contribuir con el incremento del buen estado de la red vial nacional primaria del país, posibilitando el

[12] Serna Gómez. Humberto. Gerencia Estratégica. Teoría – Metodología – alineamiento, mapas estratégicos. Octava Edición. Editorial 3R Editores. Bogotá. 2003

desarrollo de infraestructura intermodal, la conectividad e integración de la infraestructura y el cierre de brechas regionales propiciando la diversificación productiva y la competitividad del país[13].

Enmarcado en los principios de buen gobierno y de acuerdo con lo dispuesto por el Sistema Integrado de Planeación y Gestión mediante el Decreto 2482 del 3 de diciembre de 2012, en el cual se establecen los lineamientos generales para la integración de la planeación y la gestión a través de la definición de 5 políticas de desarrollo administrativo: Gestión misional y de gobierno, Transparencia, participación y servicio al ciudadano, Gestión del talento humano, Eficiencia administrativa, y Gestión financiera.

A continuación, se presenta el esquema de direccionamiento estratégico y el marco normativo con el cual se orienta la gestión institucional.

El plan Estratégico Institucional del Instituto Nacional de Vías, se rige por el Plan Nacional de Desarrollo 2014-2018, ley 1753 del 9 de junio de 2015 y las demás normas aplicables a la planeación, entre ellas:

- Artículo 341 de la Constitución Política de 1.991
- Ley 152 de 1994, Artículos 26 y 29: Establece que tras la aprobación del Plan Nacional de Desarrollo de cada gobierno se formulará con base en él los Planes de Acción de cada una de los organismos públicos y deberá efectuarse la evaluación de las metas e indicadores allí dispuestos.
- Ley 489 de 1998, Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional.

[13] plan estratégico institucional 2015-2018 - INVIAS

- Ley 1474 de 2011, Artículo 74: Por el cual se establece que todas las entidades del Estado a más tardar el 31 de enero de cada año deben publicar en la página web el plan de acción.

- Decreto Ley 019 de 2012, Artículo 233: establece que las entidades públicas están obligadas a formular y publicar los planes de acción sectoriales e institucionales a más tardar el 31 de enero de cada vigencia.

- Decreto 2482 de 2012: Establece los lineamientos para la integración de la planeación y la gestión de las entidades de la Rama Ejecutiva del Poder Público del orden nacional mediante la adopción del Modelo Integrado de Planeación y Gestión.

- Resolución 3320 de 2014: Por la cual se adopta el Modelo Integrado de Planeación y Gestión en el Instituto Nacional de Vías, se conforma el Comité Institucional de Desarrollo Administrativo y se deroga la resolución 1703 del 18 de abril de 2013.

- Dentro del plan nacional de desarrollo el Invias trabajara igualmente aparte de la inversión en vías, el desarrollo de las tecnología e información (CTI), donde se establecen como objetivos la reglamentación técnica y las acciones de modernización e innovación aplicables a la infraestructura de transporte para lograr unas vías sostenibles.

- De acuerdo a los objetivos planteados para el sector transporte entre los años 2014 - 2018, uno de los logros a alcanzar, tiene que ver con:
- La implementación de sistemas inteligentes de transporte, así como con la política de seguridad vial.

- El Decreto No. 2618 de 2013 estableció la función de “Administrar el sistema de estadísticas y mantener un inventario actualizado del estado de la infraestructura, índices de accidentalidad, costos de insumos y precios

unitarios…". En tal sentido, se ha venido trabajando en la implementación y operación del Sistema de Información Vial, así como en la consolidación y generación de información relacionada con la infraestructura de la red nacional de carreteras no concesionada, a través del proyecto "Implementación del Sistema de Gestión Integral de Riesgo en las redes de transporte en Colombia", se ha obtenido en los siguientes logros en los últimos años:

Como la información en el instituto Nacional de Vías- INVIAS, se ha convertido no sólo en un activo valioso, sino también estratégico en las organizaciones actuales del estado, no solo como medio de consulta sino también el de atender directamente al ciudadano en los procedimientos y alineamientos de la información que se maneja a nivel nacional como internacional, y cada uno de los proyectos en construcción o estudios de los mismos actualizado y a la mano.

Las bondades que ofrece un sistema de información seguro, confiable y viable acreditan a la entidad en relación al manejo y almacenamiento del activo informático, por ejemplo, al procesar información económica de la entidad mediante los sistemas de información y la nación en general (Planeación y Ministerio de Hacienda pública), como es el SIIF NACIÓN, con una precisión tal, que podría incluso diagnosticarse, en términos de tiempo, la situación de insolvencia o iliquidez, de un proyecto de inversión a grande escala o el estado financiero de la misma.

Así pues, teniendo la oportunidad de realizar el punto de partida como es el análisis de la situación real del proyecto en la acudiendo desde luego a los conceptos de Información y Seguridad, para lo cual se tendrá en cuenta las definiciones otorgadas de conceptos básicos de seguridad de la información, permiten ampliar o precisar sobre las Políticas que sobre "Seguridad de la Información", para luego así concluir el valor que tiene la información y los mecanismos para garantizar su buen funcionamiento.

Es así como los riesgos y responsabilidades de los entes estatales como en el caso del Instituto Nacional de Vías. INVIAS, conlleva a tomar en cuenta y tener siempre presente el concepto de seguridad, implementando la actualización de las existentes y navegando en nuevas para que con el indebido tratamiento de la información los activos informáticos no sean frágiles y estén prestos a un sistema de gestión de la seguridad de la información, con calidad, eficacia y eficiencia.

8.3. MARCO CONCEPTUAL

Informe de la terminología empleada dentro de este marco de referencia y utilizados durante el desarrollo del proyecto:

- **Centro De Cómputo**: Zona específica acondicionada eléctrica y ambientalmente, para el procesamiento de datos, en conexión a través de una red.
- **Confidencialidad**. Seguridad de que la información no será mostrada o expuesta a entidades no autorizadas o personas ajenas a ella o a través de controles no adecuados.
- **Integridad.** Protección y manejo provisto solamente por el personal autorizado en forma controlada, suministrando las metodologías de seguridad, para salvaguardar la información o activos informáticos, garantizando la modificación, borrado, manipulación y el almacenamiento de los archivos de forma segura.
- **Amenaza**. Evento que posibilita la ocurrencia de un incidente que cause o no un daño a la información de la entidad, originado por factores externos a la organización.
- **Vulnerabilidad.** Factor interno generado de una clase de incapacidad para anticipar, asimilar y recuperar un evento natural o acto humano inherente a

un activo de información o factor externo no controlable que constituye fuente de riesgo o amenaza.

- **Riesgo.** Acontecimiento que puede alcanzar un nivel de alto o bajo según corresponda y que sucede cuando la vulnerabilidad y la amenaza actúan juntas, generando un posible daño (material, informático, estructural o humano).

- **Control:** Acción o proceso que se encauza a la mejora o prevención de un Riesgo, bajo una guía o proceso administrativo, tecnológico físico o legal.

- **Disponibilidad.** Garantía que emite el sistema para el acceso, control y modificación de archivos o la eliminación de registros, basados en la identificación del usuario autorizado, mediante clave de acceso cuando lo requieren.

- **Trazabilidad.** Capacidad de un sistema de información para marcar y determinar quién hace y en qué momento, una actividad, con el objetivo de analizar incidentes, detectar ataques y aprender a prevenirlos en el futuro. Se materializa en la integridad de los registros de actividad.

- **Autenticidad.** Capacidad para determinar, verificar y garantizar las fuentes de la que proceden los datos, origen o el contenido de los mismos.

- **Seguridad de la Información:** Medidas preventivas y de reacción establecidas en la entidad, entre las que se pueden mencionar políticas, normas, procedimientos, estructura organizacional, así como controles tecnológicos y físicos, permitiendo el resguardado, protección, confidencialidad, disponibilidad e integridad de la información institucional.

- **SGSI**: Sistema de Gestión de Seguridad de la Información.

8.4. MARCO LEGAL

Aborda la normatividad vigente para el estudio, en lo referente a tener un histórico de los efectos administrativos y económicos para lograr una acción protagónica de las normas; efecto dinámico de las Políticas de Seguridad de la Información, al interior de la entidad, Instituto Nacional de Vías INVIAS, planta Central.

En materia de directrices para el diagnóstico de las políticas de seguridad, La Oficina Asesora de Planeación lidera el desarrollo tecnológico en INVIAS y Ejecuta las Políticas de Gobierno en materia de Tecnologías de Información y de Comunicaciones.

El Instituto Nacional de Vías. INVIAS cuenta con el "Documento Conpes No. 3854" del Consejo Nacional de Política Económica y Social de la Republica de Colombia, Departamento Nacional de Planeación, el cual pone en marcha el plan de acción y mejora de las acciones que se ejecutaran durante los años 2016 a 2019.[14]

a) Decreto 2618 de 2013, modificó la estructura del INVIAS y estableció funciones[15].
b) Resolución: No. 01363 de marzo 02 de 2016 Por la cual se adoptan las políticas establecidas en el Modelo de Seguridad y Privacidad de la Información, en el marco de la Estrategia de Gobierno en Línea[16].
c) Resolución: No.01364 de marzo 02 de 2016 Por la cual se adopta Manual de Políticas y Normas de Seguridad de la Información dentro del marco de la

[14] Departamento Nacional de Planeación. DNP
https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf
https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854_Adenda1.pdf
[15] INVIAS. https://www.invias.gov.co/index.php/servicios-al-ciudadano/normatividad/resoluciones-circulares-otros/3570-decreto-2618-2013.
[16] Invias. https://www.invias.gov.co/index.php/servicios-al-ciudadano/normatividad/resoluciones-circulares-otros?s5_responsive_switch_2002120196invias=1&start=180&limit=20&limitstart=500

Estrategia de Gobierno en Línea[17].

d) ETICOM-MN-6 Manual de Políticas y Normas de Seguridad de la Información de diciembre 10 de 2015.

e) Decreto 1078 de 2015 Estrategia de Gobierno en Línea[18].

f) ISO 27001: 2013 Sistema de Gestión de Seguridad de la Información[19].

Otros documentos como:

Norma

g) Circular Externa 002 del 6 de marzo de 2012. Comunicaciones, Tics y Manejo de la Información. Gestión Documental.

h) Resolución 265 DE 2018.

i) Resolución 2355 de 2018, Por la cual se ajusta el Comité Institucional de Control Interno.

j) Resolución 3643 de 2018, modifica la Resolución 2355 de 2018

Decreto

k) Decreto 2573 del 12 Diciembre de 2014 Estrategia Gobierno en Línea.

l) Decreto No. 1377 del 27-06-2013. Se reglamenta parcialmente la Ley No. 1581-2012 (Régimen General de Protección de Datos Personales) Derogado Parcialmente por el Decreto No. 1081-2015.

m) Decreto 1078 del 26 de Mayo 2015 Estrategia Gobierno en Línea.

n) Decreto 1008 de 2018 Gobierno Digital.

o) Decreto 415 De 2016 - CIO

De esta forma es necesario revisar la normatividad que rige a la entidad Instituto Nacional de Vías. INVIAS, a fin de determinar cuáles no se aplican correctamente.

[17] INVIAS. https://www.invias.gov.co/index.php/archivo-y-documentos/cnsc/evidencias-furag-2017/6789-pr3-adquisicion-desarrollo-y-mantenimiento-de-sistemas-de-informacion/file
[18] GEL. Link. http://estrategia.gobiernoenlinea.gov.co/623/articles-7941_manualGEL.pdf
[19] ISO. Link: http://www.iso27000.es/download/doc_sgsi_all.pdf

9. METODOLOGÍA DE LA INVESTIGACIÓN

9.1. TIPO DE INVESTIGACIÓN.

El trabajo se desarrollará como investigación aplicada, a través de trabajo de campo, en la sede central del INVIAS-Bogotá. Para el levantamiento de información se basará en la recolección de información de fuentes primarias, con entrevistas a analistas de sistemas y administradores de información.

9.2. FUENTES DE INFORMACIÓN

Se revisan dentro del contexto estratégico organizacional e incorporan mejoras en la Caracterización de proceso y demás escritos en relación con la Gestión de las Tecnología de la Información y Comunicación (Alineación GEL y seguridad de la información).

9.2.1. Primarias, Gestión de Tecnologías De La Información Y Comunicaciones. Formatos

9.2.2. ETICOM-ABC-1 - ABC De Comunicaciones - V1 Caracterización.

9.2.3. ETICOM-CP-1 – Gestión de Tecnologías de La Información Y Comunicaciones - V2.

9.2.4. ETICOM-FR-1 - ETICOM-FR-1 Control De Acceso Al Centro De Cómputo - V1

Guía- Instructivo

9.2.5. ETICOM-IN-1 - Control De Acceso Al Centro De Cómputo - V1

Instructivos del Manual de Interventoría

Manual

9.2.6. Eticom-Mn-1 - Manual De Uso Aranda Service Desk Web Edition Para Usuarios - V1

9.2.7. Eticom-Mn-6 - Manual de Políticas Y Normas De Seguridad en la Información - V1

Planes- Políticas

9.2.8. Procedimiento

9.2.9. Eticom-Pr-1 - Adquisición Mantenimiento Y Actualización De La Plataforma Tecnológica - V1

9.2.10. Eticom-Pr-2 - Soporte Tecnológico - V1

9.2.11. Eticom-Pr-3 – Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.- V1

9.2.12. Eticom-Pr-4 - Planeación Servicios Tecnológicos - V1

9.2.13. Eticom-Pr-5 - Creación Y/O Activación De Cuentas De Usuario - V1

9.2.14. Eticom-Pr-6 - Administración Antivirus - V1

9.2.15. Eticom-Pr-7 - Copia De Seguridad De Usuario Final - V1

9.2.16. Eticom-Pr-8 - Comunicación Institucional - V1

9.2.17. Eticom-Pr-9 - Eliminación Segura De Información En Equipos De Usuario Final - V1

Protocolo- Registro

9.2.18. Tablas De Retención Documental

9.2.19. Documentos Externos

9.2.20. Formato De Cliente

Norma

9.2.21. Circular Externa 002 Del 6 De Marzo De 2012

Ley

9.2.22. Resolución

9.2.23. Resolución 265 De 2018

9.2.24. Resolución 2355 De 2018, Por La Cual Se Ajusta El Comité Institucional De Control Interno

9.2.25. Resolución 3643 De 2018, Modifica La Resolución 2355 De 2018

Decreto

9.2.26. Decreto 2573 Del 12 Diciembre De 2014 Estrategia Gobierno En Línea

9.2.27. Decreto 1377 Del 27 De Junio De 2013

9.2.28. Decreto 1078 Del 26 De Mayo 2015 Estrategia Gobierno En Línea

9.2.29. Decreto 1008 De 2018 Gobierno Digital

9.2.30. Decreto 415 De 2016 - Cio

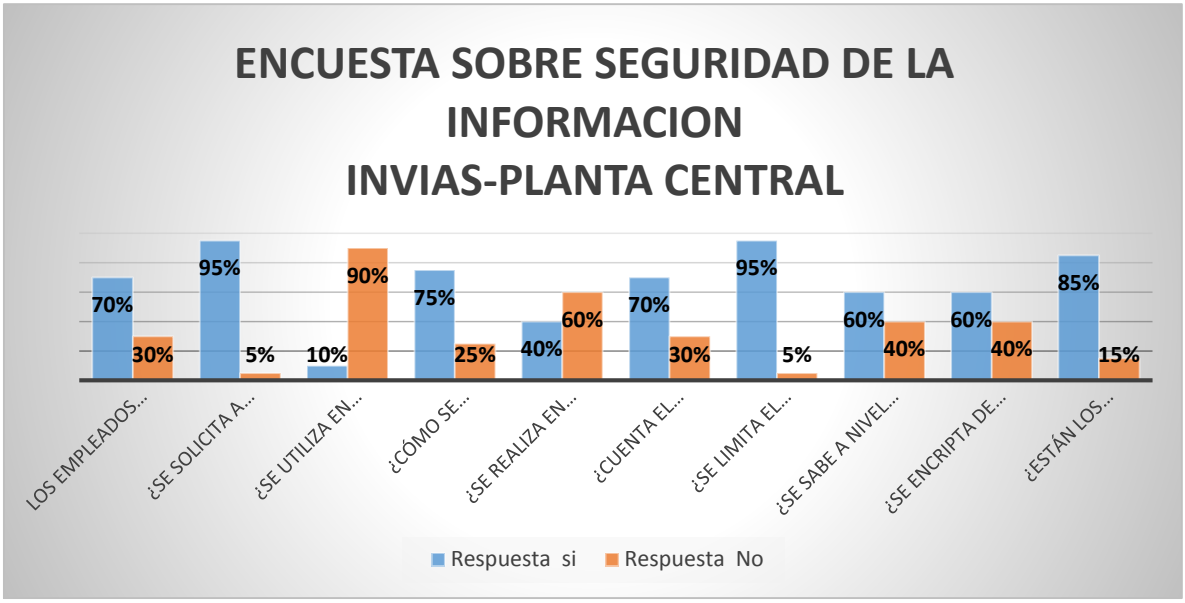
Dado que la investigación que se proyecta es de carácter cualitativo, se empleara medios como la entrevista, la observación, un cuestionario de preguntas abiertas, bitácoras y diarios, etc. Será la técnica que se presente para el tipo de datos que se están solicitando en el estudio.

Tabla 1. Preguntas y evaluación

PREGUNTA	Respuesta	
	si	No
Los Empleados del INVIAS-Planta Central utilizan una contraseña fuerte, para el ingreso obligatorio a las fuentes y bases de Datos de información?	70%	30%
¿Se Solicita a los Funcionarios-Contratistas que cambien las contraseñas con regularidad?	95%	5%
¿Se Utiliza en el Invias-Planta Central un sistema de autenticación de doble factor?	10%	90%
¿Cómo se integran los Dispositivos celulares, de los empleados o directivos a la red del INVIAS, en planta central?	75%	25%
¿Se realiza en el Invias-Planta Central una copia periódica sobre la Información y seguridad de la información o Datos de la entidad en planta central?	40%	60%
¿Cuenta el INVIAS-Planta central con las soluciones de seguridad adecuadas?	70%	30%
¿Se Limita el número de Funcionarios de Planta Central en el INVIAS que tienen privilegios de administrador en la infraestructura IT?	95%	5%
¿Se sabe a nivel de funcionario de la entidad-planta central reconocer un e-mail sospechoso?	60%	40%
¿Se encripta de alguna manera las BD, del Invias-Planta Central y la información sobre los clientes?	60%	40%
¿Están los sitios web de la entidad INVIAS-Planta central protegidos?	85%	15%

Fuente: Instituto Nacional de Vías. INVIAS

Figura 4. Resultados gráficos de la Encuesta sobre Seguridad de la Información en el Instituto Nacional de Vías. INVIAS



Fuente: Instituto Nacional de Vías. INVIAS

Mencionados todos ellos de forma claramente verbal por el ingeniero a cargo de los procesos en la plataforma tecnológica para la comprensión de cada uno de los procesos que se toman, ante las situaciones propias de estos colaboradores en los contextos, ya estratégicamente estudiados y evaluados. Y se ha comprobado que entre más se conoce la ideología de un WannaCry y otros ataques informáticos que recientemente han atacado plataformas de información importantes en el país (Zonas Bancarias), han demostrado que la seguridad es un papel cada vez más importante.

No solo ayuda económicamente a tomar terreno para la adquisición de las mejores y sofisticados medidas defensivas y adecuadas, sino que hoy día es una opción que no solo basta con tenerla para solucionar problemas de seguridad informática, sino que en última instancia, sólo es una buena política de formación en seguridad IT orientada así los funcionarios que aprenden sobre la protección de los datos y de los activos informáticos del INVIAS-Planta Central.

10. DESARROLLO DE LA METODOLOGÍA DE LA INVESTIGACIÓN

Una vez dado los resultados de la investigación y aplicada a la dinámica de sistemas, este proyecto se realiza en cuatro fases, orientadas a la explicación de los objetivos propuestos bajo un enfoque metodológico que alcanza a analizar y proponen, las mejoras al “Manual de Políticas de Seguridad de la Información del Institutito Nacional de Vías. INVIAS, planta central.”

a) **La primera fase** analiza la documentación, identifica los activos informáticos de la entidad, INVIAS, la documentación con la información que se relaciona con la temática propuesta de investigación del tema, como todos aquellos procedimientos, normas, leyes, resoluciones, políticas implementadas que rigen para la entidad.

   El análisis anterior contempló datos como: número de usuarios, servidores, terminales de trabajo, software, licencias etc. Soporte de la información mediante entrevista al ingeniero de soporte tecnológico, sobre virtudes y falencias del sistema, la estructura e infraestructura tecnológica, los riesgos sobre seguridad física y del entorno de la seguridad informática, el crecimiento de la infraestructura de la entidad, Instituto Nacional de Vías, INVIAS. Todo esto como base para la generación de las nuevas Políticas de Seguridad de la Información, aprobadas por la alta dirección de la entidad.

   Anexo A. Activos Informáticos Del Instituto Nacional De Vías- INVIAS.

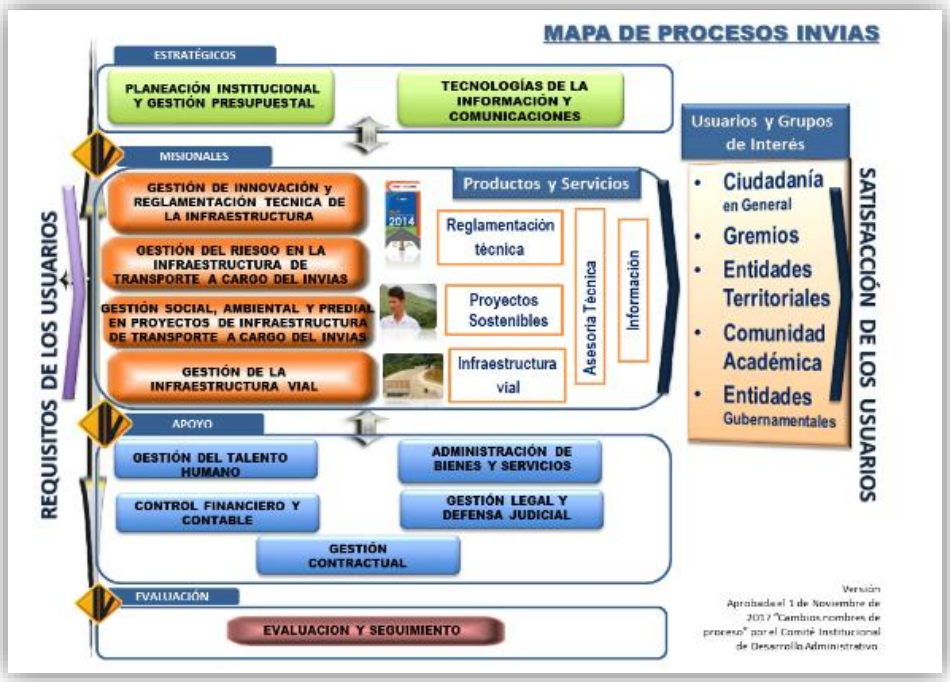
b) **La segunda Fase**: Se Generó, Organizo y tabulo, lo referente a la información recolectada sobre la infraestructura informática y la información, para el diagnóstico inicial. Igualmente los factores de amenazas y protecciones utilizadas, el mapa de procesos de la Entidad Instituto Nacional de Vías-INVIAS y la documentación jurídica, como también lo existente frente a la norma NTC 27000 y la estrategia GEL.

- **MAPA DE PROCESOS**

El área de Informática se encuentra en los planes estratégicos de la Entidad y Coordinada por la Oficina Asesora de Planeación. Igualmente las directrices están dadas en el Manual de Funciones de la entidad, su distribución y tareas a realizar.

Dentro del mapa de procesos la oficina tiene como Objetivo “liderar y Gestionar los servicios de Tecnología de la Información y Comunicación, garantizando así la disponibilidad, divulgación y seguridad de la información, cuando de tomar decisiones se trate en cumplimiento de la Misión y estrategias del Institutito Nacional de Vías. INVIAS. En interacción e interoperación de información con la ciudadanía en general y de otras entidades del estado.

Figura 5. Mapa de Procesos de la entidad Instituto Nacional de Vías. INVIAS.



Fuente. INVIAS. Versión aprobada 1-11-2017 “Cambio nombre de procesos”, por el comité Institucional de Desarrollo Administrativo”.

- **DOCUMENTACIÓN JURÍDICA**

Decretos

- Decreto 2573 del 12 Diciembre de 2014 Estrategia Gobierno en Línea
- Decreto 2482 del 03-12-2012 Se establecen los lineamientos generales integrales de la Planeación y la Gestión.
- El Decreto No. 1377 del 27-06-2013
- Decreto 1078 del 26 de Mayo 2015 Estrategia Gobierno en Línea.

Anexo B. Categorías De Los Activos Las Vulnerabilidades, Amenazas De Seguridad Encontrados En el INVIAS.

Figura 6. Valoración De Los Activos (Matriz de Riesgos y Evaluación)

Análisis de Riesgo promedio

		Probabilidad de Amenaza							
		Daño físico	Eventos naturales	Perdida de los servicios esenciales	Perturbación debida a la radiación	Compromiso de la información	Falla Tecnica	Acciones no autorizadas	Compromiso de las funciones
IMPORTANCIA (Magnitud de Daño)	SOFTWARE	7,8	3,8	11,0	5,9	9,0	9,3	8,8	8,3
	BASE DE DATOS - Instancias	7,9	3,9	11,1	7,6	9,1	9,4	8,9	8,3
	INFRAESTRUCTURA TECNOLOGICA	9,1	4,5	12,8	9,2	10,5	10,9	10,2	9,6
	INFRAESTRUCTURA FISICA Y DEL ENTORNO	10,3	5,1	14,5	7,2	11,8	12,3	11,6	10,9
	RED - Comunicaciones	12,3	6,1	17,3	8,7	14,2	14,7	13,9	13,0
	PERSONAL	10,7	5,3	15,1	7,5	12,3	12,8	12,1	11,3
	DOCUMENTOS FISICOS Y/O MAGNETICOS	8,5	4,2	12,0	6,0	9,8	10,2	9,6	9,0

Fuente: Instituto Nacional de Vías. INVIAS, Planta Central

PROBABILIDAD DE IMPACTOS Y RIESGOS. ANÁLISIS DE EVALUACIÓN.

1. Obsolescencia tecnológica por falta de actualización en el software y/o hardware o carencia de soporte por los proveedores, diferentes fuentes de software que demandan múltiples servicios de expertos externos por limitación interna de especialidad; implicando incompatibilidad con nuevas tecnologías (software y hardware) y un latente colapso total de la plataforma tecnológica

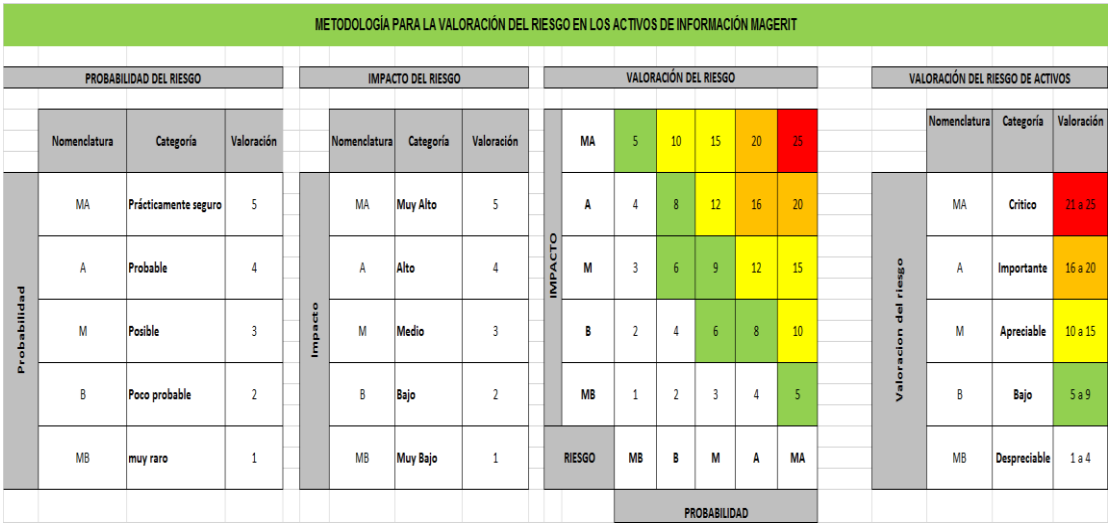
2. Obsolescencia de la versiones de las bases de datos, pérdida de soporte por parte del fabricante dada la antigüedad de las versiones, proximidad al límite de la capacidad de almacenamiento y/o múltiples contenedores de las bases de datos ocasionando posibles pérdida de información de la base de datos e imposibilidad de recuperar la información.

3. Dificultad para atender oportunamente una situación crítica, por ausencia de protocolos, inexistencia de redundancia a nivel de: bases de datos, red y/o funciones de expertos (internos y externos), disminuyendo la capacidad de reacción y continuidad del negocio.

4. Deficiencias en la recuperación de la información a partir de las copias de seguridad, debido a la falta de soporte de los proveedores del software y hardware empleado en esta actividad, así como falta de experticia en la administración de la herramienta existente, límites de la capacidad de almacenamiento y/o deficiencias en la custodia de las de dichas copias; dificultando la oportuna toma de decisiones y generando desgaste administrativo y reproceso dentro de la entidad

5. Deficiente personal para cubrir el 100% los roles y actividades a cargo del Grupo de TI, la estructura actual tiene 4 nivel Profesional, 4 personas Analistas, 8 personas Nivel Asistencial y 6 personas Contratistas, (2 profesionales y 4 asistenciales); total 22 personas

Figura 7. Metodología Magerit para Valoración del Riesgo- Instituto Nacional de Vías. INVIAS



METODOLOGÍA PARA LA VALORACIÓN DEL RIESGO EN LOS ACTIVOS DE INFORMACIÓN MAGERIT

PROBABILIDAD DEL RIESGO

	Nomenclatura	Categoría	Valoración
Probabilidad	MA	Prácticamente seguro	5
	A	Probable	4
	M	Posible	3
	B	Poco probable	2
	MB	muy raro	1

IMPACTO DEL RIESGO

	Nomenclatura	Categoría	Valoración
Impacto	MA	Muy Alto	5
	A	Alto	4
	M	Medio	3
	B	Bajo	2
	MB	Muy Bajo	1

VALORACIÓN DEL RIESGO

IMPACTO						
	MA	5	10	15	20	25
	A	4	8	12	16	20
	M	3	6	9	12	15
	B	2	4	6	8	10
	MB	1	2	3	4	5
RIESGO		MB	B	M	A	MA
		PROBABILIDAD				

VALORACIÓN DEL RIESGO DE ACTIVOS

	Nomenclatura	Categoría	Valoración
Valoracion del riesgo	MA	Critico	21 a 25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Fuente: Instituto Nacional de Vías. INVIAS.

Anexo C. Vulnerabilidades, Amenazas De Seguridad Encontrados En el Instituto Nacional de Vías- INVIAS- Nivel Planta Central.

- **IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN**

  a) **Información**: Contiene toda la información física y virtual creada por la entidad, Instituto Nacional de Vías. INVIAS.

  b) **Sistemas**: Todos los sistemas informáticos diseñados por la entidad Instituto Nacional de vías INVIAS

  c) **Tecnología**: Es todo el hardware y software que permite la ejecución de proceso y almacenamiento de la información.

  d) **Personas**: Es el recurso humano adscrito a la entidad Instituto Nacional de vías INVIAS para ejercer su función.

  e) **Estructural**: edificaciones de todas las unidades ejecutoras de la entidad Instituto Nacional de vías INVIAS.

Tabla 2. Vulnerabilidades, Amenazas Y Riesgos De Seguridad De Cada Activo Y Servicios De Red Relacionado- Instituto Nacional de Vías-INVIAS-Planta Central.

Activo	Amenaza	Riesgo	Descripción del Riesgo
Aire Acondicionado Centro de Cableado	Falla o Daño del Equipo	Afectación del Servicio	puede causar afectación de los equipos de red , en relación a la elevada configuración de temperatura en el centro de computo
Bases de datos de Protección	Claves débiles o compartidas	Integridad de la información o perdida de la misma	Claves débiles por parte de los usuarios, que afecten la integridad de la información y la confiabilidad de la misma
Cableado Estructurado	Personal No autorizado	Afectación del Servicio.	Daños o usado con fines de no a la entidad.
Cisco Catalyst4500 Series Switches	Perdida de Información	Denegación del Servicio	Si se daña un swtich, no se establecen los servicios de red
Rúters Cisco DPC 2425	Falla o daño del equipo	Denegación del Servicio	No se cuenta con reacción inmediata para un nuevo Rúters en caso de daño o falla.
Servidor para el DHCP, DNS	Abuso de derechos de Administración	Acceso de personal no autorizado	ingreso al servidor y modificar información de los puntos ejecutables de los módulos de seguridad
UPS 30 KVA	Falla o Daño del Equipo	Afectación del Servicio	Inconvenientes con los equipos de red y servidores en caso de cortes de fluido eléctrico.
Equipos de computo	Software no deseado	Causar daño o pérdida total o integral de la información	infestación de los equipos por virus a través de hardware externo (memorias, Discos duros extraíbles Teléfonos celulares, etc.
Impresoras y Escáner	Manejo inadecuado	Perdida de confidencialidad de la Información y Desconfiguración o daño del Hardware	Personal no autorizado o con falta de capacitación en su manejo

Fuente: Instituto Nacional de Vías. INVIAS.

La información que se maneja en la entidad Instituto Nacional de Vías. INVIAS-Planta Central, es un bien muy importante, que como cualquier otro activo de la entidad, en consecuencia necesita ser debidamente protegida.

Tabla 3. Clasificación de los Niveles de Protección de la Información, en el Instituto Nacional de Vías. INVIAS.

CONFIDENCIALIDAD	**ALTA**	El instituto Nacional de Vías –INVIAS, establece los requisitos tanto legales como aquellas que se general de una obligación contractual, que se tienen en cuenta con terceros o con el personal provisto. Incluyendo temas de oportunidad en las Políticas de Seguridad, acuerdos o clausulas para el intercambio de la información y/o acuerdos cláusulas de confidencialidad.
	MEDIA	El instituto Nacional de Vías –INVIAS, Implanta y comunica normas y responsabilidades frente a la seguridad de la Información, que le competen al personal provisto que cuenta con acceso a la plataforma tecnológica o la información.
	BAJA	Información que se maneja en El instituto Nacional de Vías –INVIAS, puede entregarse o ser publicada acorde a los fueros que le otorgue la calidad de restrictivo, y solicitada mediante oficio, puede ser consultada sin que esto signifique daño alguno a las procesos y actividades dentro de la entidad.
	NO CLASIFICADA	El instituto Nacional de Vías –INVIAS, Monitorea los Acuerdos de Niveles de Servicio en cumplimiento de los acuerdos y a entera satisfacción de los usuarios frente a estos, con el objetivo de proponer mejoras sobre los mismos.
INTEGRIDAD	**ALTA**	El instituto Nacional de Vías –INVIAS, mide la disponibilidad e integridad de la información, a través de copias generadas de respaldo y pruebas de restauración, garantizando de esta forma si hay fallas del sistema , sin que esto afecte los demás procesos identificados y que se realicen en la plataforma tecnológica.
	MEDIA	Divulgar y establecer por parte del Instituto Nacional de Vías. INVIAS, los procedimientos de copiado respaldo junto con el formato asociado.
	BAJA	Se define el sitio de custodia externa. Teniendo en cuenta la importancia de la información guardada en el tiempo y los requisitos legales, que sean necesarios y la normatividad vigente que apliqué para el Instituto Nacional de Vías-INVIAS- Planta Central.
	NO CLASIFICADA	Se evalúa la necesidad de instaurar los controles criptográficos a las documentos y copias de respaldo, considerando los requerimientos legales aplicables al Instituto Nacional de Vías –INVIAS.
DISPONIBILIDAD	**ALTA**	La información debe estar disponible a través de la generación de copias de respaldo físicas, si hay falla del servicio sin que este afecté la plataforma tecnológica del Instituto Nacional de Vías INVIAS.
	MEDIA	Los activos informáticos del Institutito Nacional de Vías., INVIAS, son un medio de identificación, categorización y priorización de los procesos misionales de la misma, por lo que se hace necesario evaluar su disponibilidad dentro de la entidad.
	BAJA	El Instituto Nacional de Vías. INVIAS-planta central, elabora los planes de auditoria y fija cual realizara bajo coordinación del equipo auditor, las fechas previstas para llevarla a cabo, como también la documentación de referencia y las personas que deben participar en ella.

Fuente: Instituto Nacional de Vías. INVIAS

Tabla 4. Inventario De Activos de la Información[20].

Activos	Cantidad
Infraestructura Físicos	39
Red de Comunicaciones	4
Personal	10
Físico-Electrónico	1
Infraestructura-Física del Entorno	7
Digitales	56
Software (aplicativos)	40
Base de Datos	9
Total	166

Fuente: Instituto Nacional de Vías. INVIAS

Corresponde al inventario de la información pública del Instituto Nacional de Vías. INVIAS información que se encuentra a disposición en forma impresa y escrita y que puede ser transmitida por cualquier medio electrónico o almacenada en equipos de cómputo, incluyendo datos contenidos en registros, archivos, bases de datos, videos e imágenes

Anexo D. LISTAS DE CHEQUEO PARA VERIFICACIÓN

Contiene el cumplimiento de la Norma ISO/IEC 27002, de los controles y de acuerdo al nivel de madurez o grado de cumplimiento en (%).

[20] Instituto Nacional de Vías. INVIAS. INVIAS. https://www.invias.gov.co/index.php/servicios-al-ciudadano/inventario-de-informacion

Figura 8. Validación Del Modelo. Invias

PORCENTAJE TOTAL DE REQUISITOS		77%	80%
Ítem	Aspectos Requeridos del SGSI	GAP Inicial	GAP Final
4	CONTEXTO DE LA ORGANIZACIÓN	80%	80%
4,1	CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO	80%	80%
4,2	COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS	80%	80%
4,3	DETERMINACIÓN DEL ALCANCE DEL SGSI (El alcance debe estar disponible como información documentada.)	80%	80%
4,4	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	80%	80%
5	LIDERAZGO	79%	80%
5,1	LIDERAZGO Y COMPROMISO	80%	80%
5,2	POLÍTICA	77%	80%
5,3	ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZAC	80%	80%
6	PLANIFICACIÓN	71%	80%
6,1	ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES	62%	80%
6,2	OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y PLANES PARA LOGRARLOS	80%	80%
7	SOPORTE	74%	79%
7,1	RECURSOS	80%	80%
7,2	COMPETENCIA Las acciones aplicables pueden incluir, por ejemplo: la formación, la tutoría o la reasignación de las personas empleadas actualmente; o la contratación de personas competentes.	75%	75%
7,3	TOMA DE CONCIENCIA	80%	80%
7,4	COMUNICACIÓN	60%	80%
7,5	INFORMACIÓN DOCUMENTADA La información documentada de origen externo, que la organización ha determinado que es necesaria para la planificación y operación del sistema de gestión de la seguridad de la información, se debe identificar y controlar, según sea adecuado. NOTA El acceso implica una decisión concerniente al permiso solamente para consultar la información documentada, o el permiso y la autoridad para consultar y modificar la información documentada, etc.	80%	80%
8	OPERACIÓN	73%	80%
8,1	PLANIFICACIÓN Y CONTROL OPERACIONAL La organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos y para implementar las acciones determinadas en el apartado 6.1. La organización también debe implementar planes para lograr los objetivos de la seguridad de la información determinados en el apartado 6.2.	60%	80%
8,2	EVALUACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN La organización debe llevar a cabo evaluaciones de riesgos de la seguridad de la información a intervalos planificados o cuando se propongan u ocurran cambios significativos, teniendo en cuenta los criterios establecidos en el apartado 6.1.2 a)	80%	80%
8,3	TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓ	80%	80%
9	EVALUACIÓN DEL DESEMPEÑO	80%	80%
9,1	SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN La organización debe conservar información documentada apropiada como evidencia de los resultados del monitoreo y de la medición.	80%	80%
9,2	AUDITORÍA INTERNA La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca del SGSI Los programas de auditoría deben tener en cuenta la importancia de los procesos involucrados y los resultados de las auditorías previas	80%	80%
9,3	REVISIÓN POR LA DIRECCIÓN La alta dirección debe revisar el sistema de gestión de la seguridad de la información de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia continuas. Los elementos de salida de la revisión por la dirección deben incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio en el sistema de gestión de la seguridad de la información. La organización debe conservar información documentada como evidencia de los resultados de las revisiones por la dirección.	80%	80%
10	MEJORA	80%	80%
10,1	NO CONFORMIDADES Y ACCIONES CORRECTIVAS	80%	80%
10,2	MEJORA CONTINUA	80%	80%

Fuente: Instituto Nacional de Vías. INVIAS.

Figura 9. Aspectos Requeridos del SGSI Modelo. INVIAS-planta central

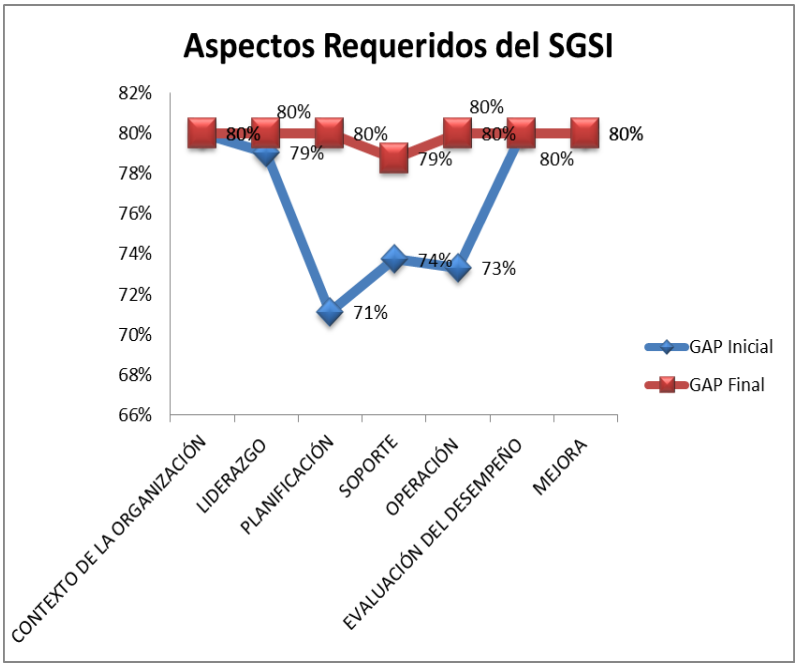
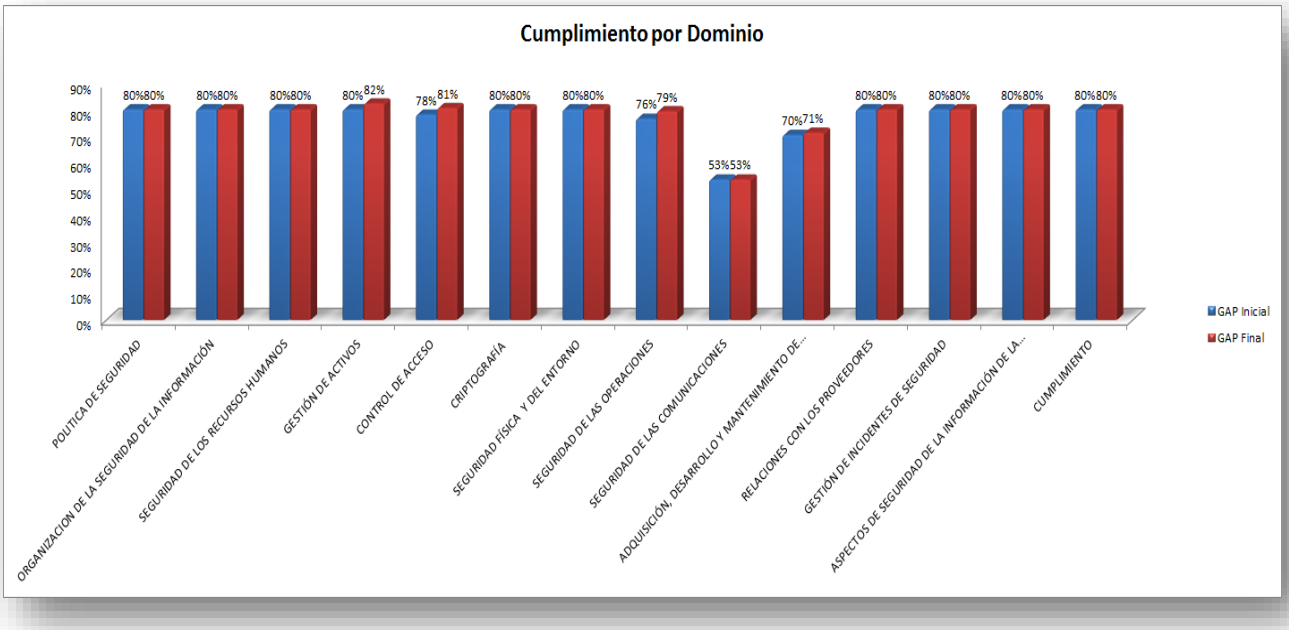


Figura 10. Gráfico Consolidación cumplimiento Norma ISO/IEC 27002 referente controles, con nivel de madurez o grado de cumplimiento (%), modelo INVIAS - Planta Central.



Fuente: Instituto Nacional de Vías. INVIAS.

c) **La tercera Fase**: Diagnostico de las “Políticas”, identificando la existente**,** el manejo de la misma y la seguridad de la información, asumiendo tareas de identificación y clasificación de las mismas.

- **POLÍTICAS DE RIESGO**

De acuerdo a la actual Política de administración de Riesgo, la Oficina Asesora de Planeación del Instituto Nacional de Vias. INVIAS, plata central, coordinará semestralmente el seguimiento y la actualización de las cartas de Riesgo.

La Matriz Institucional de Riesgos de Gestión consolida la información básica de las cartas de Riesgo, mientras el mapa Institucional de Riesgos de Gestión de Gestión es la representación gráfica de la criticidad de los riesgos monitoreados. Dando cumplimiento a la actividad programada en el Plan de Acción 2017 “Divulgar el mapa de Riesgos Institucional y la Política de administración del Riesgo”.

- **POLÍTICAS DE SEGURIDAD**

El Instituto Nacional de Vías. INVIAS, posee un grupo de Políticas de Segundad de la Información, revisadas y aprobadas en el año 2014, partiendo de las Políticas de Segundad y Privacidad (GEL), sugeridas por el Modelo de Seguridad y Privacidad de la Información de Gobierno en Línea en su versión anterior.

Estas políticas y sus normas asociadas serán de pertinente relevancia y aplicación al interior del Instituto Nacional de Vías. INVIAS, planta central, territoriales, sus funcionarios, contratistas, personal provisto por terceras partes y todos aquellos que son responsables sobre las fuentes y recursos

de procedimiento y procesamiento de información con responsabilidades sobre las fuentes y recursos del Instituto Nacional de Vías. INVIAS

El esquema de presentación del documento a implementar revisa el contexto estratégico organizacional e incorpora las mejoras en las características de todos los procesos mencionados del documento y relacionados con la gestión tecnológica de la entidad, en tres secciones , la primera especifica las políticas de Seguridad de la Información, la segunda integra todo el componente normativo que sobre seguridad de la información se plantea y que tiene relación directa con las políticas de seguridad de la información, tanto base como soporte de las mismas.

Una tercera que incluye a todas los niveles de seguridad en la medida que se ejecuta la política, sobre un activo informático que se va a proteger, de que protegerlo y como protegerlo, todo bajo el esquema normativo y de seguridad de la información, GEL/ISO 27000

d) **La Cuarta Fase**: relaciona las tecnologías, estándares y elaboración del documento final, en el que se toman en cuenta los diferentes grupos de la oficina de sistemas del INVIAS, tales como, Plataforma Tecnológica, Soporte y Control y Sistemas de Información, y según su organización.

- **OFICINA DE TECNOLOGIAS DE INFORMACION Y COMUNICACIONES –INVIAS- ORGANIZACIÓN.**

  i. Grupo Sistemas de la Información.

  Grupo de trabajo interdisciplinario que trabaja con el objetivo de identificar las necesidades de aplicativos que soporten los procesos de la Entidad, así como, analizar, priorizar, documentar y definir la manera de atender los desarrollos, que sean necesarios, para facilitar el trabajo a los funcionarios.

Tabla 5. Tecnologías de la Información y servicios tecnológicos de la Comunicación del Institutito Nacional de Vías. INVIAS, Planta Central.

SERVICIO	DESCRIPCIÓN	ELEMENTO
OFIMÁTICA	Son herramientas y/o recursos tecnológicos que INVIAS pone a disposición de sus colaboradores, para facilitar y optimizar el trabajo.	**OFFICE365.** Esta suite ofrece procesador de texto (Word), hoja de cálculo (Excel), diseñador de presentaciones (Power Point), mensajería instantánea (correo electrónico), videoconferencia (Skype), entre otros**.**
		AUTOCAD, ACROBAT, VISIO. El responsable de disponer lo necesario para ofrecer estos servicios es el Grupo de Plataforma Tecnológica

Fuente: Instituto Nacional de Vías. INVIAS

ii. Grupo de Plataforma Tecnológica

Se encarga de identificar las necesidades de Infraestructura tecnológica, priorizar, estructurar y adquirir los diferentes dispositivos y herramientas que la conforman, para ponerla a disposición de los sistemas de información y demás servicios tecnológicos, de tal forma que se garantice la prestación segura de todos los servicios tecnológicos a los funcionarios de INVIAS.

iii. Grupo de Soporte y Control

Recibe y atiende cada una de las solicitudes de servicios o requerimientos de los usuarios, respecto al correcto funcionamiento de los Servicios tecnológicos. Para lo cual, disponen de las extensiones telefónicas 1111 y 2222 y del correo electrónico soportesiri@invias.gov.co, para atender a los usuarios.

- **CENTRO DE CABLEADO**

Centro de acopio e instalación de los servicios de las comunicaciones de y cableado de Red física que componen la red del instituto Nacional de vías, INVIAS, planta central.

Dentro de estos centros de cableado se deben cumplir y establecer unos requisitos establecidos, como aquellos que tienen que ver con las zonas de accesos Físicos materiales para los pisos, techos y suministros eléctricos, medidores de temperatura y de humedad, igualmente.

- **CENTRO DE COMPUTO**

Franjas o sitios específicos para el alojamiento y ensamblaje de computadores, que se utilizan en el procesamiento de datos, los cuales están conectados a través de la red. El centro de cómputo debe cumplir con los estándares establecidos en la norma del SGSI, para así avalara cada uno de los controles de acceso físico, pisos y techos, condiciones medioambientales y alimentación eléctrica adecuada.

El Institutito Nacional de Vías. INVIAS, sitúa dentro de organización tecnológica, 28 aplicativos, los cuales interactúan en las tareas que realizan a diario sus colaboradores, en el desarrollo de sus tareas. A estos aplicativos se puede ingresar por la intranet institucional.

También permite a través de su plataforma tecnológica, la interacción con 6 aplicativos externos, es decir de otras entidades del gobierno, como son Min hacienda, Min transporté, DNP, etc. El responsable de analizar, priorizar y del desarrollo de estos aplicativos es el Grupo de Sistemas de Información.

- **SERVICIOS DE CONECTIVIDAD/COMUNICACIONES**

Son todos aquellos recursos tecnológicos que sin ser muy perceptibles por los usuarios, les permiten estar conectados con la Entidad a nivel nacional y con el

mundo. Les permiten comunicarse vía texto, voz y video y desarrollar su trabajo en equipo, de manera colaborativa, sin que la distancia sea una barrera.

En este grupo se encuentra el servicio de Internet, servicio de red local y corporativa, inalámbrica y alambrada, servicio de telefonía IP, para ofrecer estos servicios, la Entidad cuenta con una infraestructura tecnológica moderna, la cual, requiere de una gestión y monitoreo permanente.

Tabla 6. Atención al usuario o mesa de ayuda, Instituto Nacional de Vías- INVIAS- Planta Central.

SERVICIO	DESCRIPCIÓN	ELEMENTO
CONECTIVIDAD / COMUNICACIONES	Soporte Técnico	Corresponde al servicio de atención al usuario o mesa de ayuda, que recibe, registra y atiende las solicitudes y/o requerimientos del usuario, mediante las extensiones 1111, 2222 y el correo soportesiri@invias.gov.co. Con el fin de llevar control, estos canales son el único punto de contacto, disponible y habilitado para que el usuario haga solicitudes de soporte en INVIAS.

Fuente: Instituto Nacional de Vías. INVIAS

Para el Institutito Nacional de vías. INVIAS, planta central el compromiso de estructurar, habilitar y disponer toda la Infraestructura Tecnológica necesaria para poder ofrecer a los usuarios, los diferentes servicios tecnológicos, desde las comunicaciones, sistemas de información, hasta las herramientas de ofimática, es el Grupo de Plataforma Tecnológica.

11. RESUMEN DE RESULTADOS

11.1. En cuanto al objetivo general del proyecto, un Análisis de resultados facilita la actualización y mejora al documento Manual de Políticas y Normas de Seguridad de la Información y las comunicaciones, para el Instituto Nacional de Vías. INVIAS, planta central, una versión actualizada de los riesgos, amenazas y peligros a que se puede ver expuesta la información y los activos informáticos del Instituto Nacional Vías Invias. Y de acuerdo con el modelo MSPI y reglamentado por el Modelo de Seguridad y Privacidad de Gobierno en Línea (GEL) y los estándares actuales.

11.2. Del proceso que la entidad ha diseñado hasta el momento, el diagnóstico es concluyente, puesto que aunque coexiste una cultura sobre seguridad de la información, sobre los sistemas de Control de seguridad Informática y de la Información, sobre procesos y procedimientos que se documentan igualmente, dentro de la organización, algunos procedimientos para protección de la información, se pasan por alto y sin documentar.

11.3 Una vez se entregue esta relación como informe final, existe el compromiso real de las directivas de la entidad y los funcionarios, sobre lo que se debe y se pretende, evidenciar en el análisis de seguridad de la información, como también el hecho de que al respecto, el personal del área informática está en capacitación constante para asumir dicha responsabilidad.

11.4. Por lo tanto, el Institutito Nacional de Vías. INVIAS, planta central vista como entidad del estado, cuenta con un marco normativo de seguridad, que permita aplicar este proceso continuo de auditoría basada en la normativa ISO/IEC 27002 y de manera periódica, con auditoras externas, que le permiten hacer la evaluación y seguimiento del sistema de control de seguridad informático para el diseño, implementación e implantación de un SGSI adecuado a sus necesidades. Puesto que son la Identificación de la imagen corporativa de la entidad “Instituto Nacional de Vías INVIAS**”.**

12. RESUMEN DE LAS CONCLUSIONES

12.1. Una vez logrado el objetivo general del proyecto se trabajan los objetivos específicos los cuales plantean que una vez realizado el Análisis del Manual de Políticas y Normas de Seguridad de la Información, en el Institutito Nacional de Vías. INVIAS, planta central, se identificaron todos y cada uno de los Activos Informáticos que se van a proteger bajo el esquema normativo de seguridad GEL/ISO 27001:2013 y las áreas susceptibles de ataques o con problemas de seguridad dentro del INVIAS.

12.2. Al tener conocimiento del activo informático que se va a proteger bajo el esquema normativo de seguridad GEL/ISO 27001:2013, unas políticas actualizadas identifican las amenazas y debilidades del actual sistema de manejo y protección de la información, del Instituto Nacional De Vías. Por lo que al elaborar un diagnóstico de estas Políticas de Seguridad, Privacidad y manejo de la Información, existen con las ajustadas a estándares internacionales actuales, dará una mejor oportunidad de eficiencia y eficacia a la entidad, solucionando en buena parte los problemas de seguridad dentro del Institutito Nacional de Vías, INVIAS, planta central.

12.3. Una vez Identificas las amenazas y debilidades del actual sistema de manejo y protección de la información, en el Invias se logra diagnosticar los problemas que surgen en cuanto a la protección de la información y los activos informáticos. Por lo que las Políticas de Seguridad, Privacidad y Manejo de la Información existentes con las ajustadas a estándares internacionales actuales, se elaborara el documento final que incluya las actualizaciones, recomendaciones y formulaciones sobre Políticas de Seguridad de la Información y Comunicación, de manera tal que puedan ser

aprobadas y adaptadas por el Instituto Nacional de Vías, INVIAS, Planta central.[21].

[21] Instituto Nacional de Vías. Invias. https://www.invias.gov.co/index.php/archivo-y-documentos/cnsc/evidencias-furag-2017/6783-manual-politicas-seguridad-v1-0/file

13. RECOMENDACIONES

En este orden de ideas se recomienda ajustar de manera inmediata el actual Manual de Políticas de Seguridad, Privacidad y Manejo de la Información existentes con las ajustadas a estándares internacionales actuales. Trabajar en pro de la nueva actualización del Manual de Políticas de Seguridad de la Información, con la Dirección y la Oficina de Planeación Institucional, para así, hacer partícipe a los líderes de procesos/subprocesos en el ajuste e implementación de estas políticas, al 2018.

Se debe Instruir de manera adecuada sobre la nueva metodología Estrategias para la socialización de las Políticas de Seguridad de la Información, del Instituto Nacional de Vías. INVIAS, planta central.

El Modelo de Seguridad y Privacidad de GEL y la madurez del modelo en el INVIAS, recomienda que se debe implementar de inmediato a todos los indicadores generados en este proyecto, con el fin de generar registros en cada uno de ellos.

- Observando y monitorear los indicadores creados de acuerdo con los registros generados, con el fin de verificar si el objetivo del indicador se cumple o si el mismo requiere un ajuste de acuerdo a su comportamiento.
- Controlar el Tiempo que lleva la implementación del proyecto.
- El Dominio de la Norma ISO/IEC 27001:2013.
- Roles para llevar a cabo la implementación y/o monitoreo del presente proyecto.

- Incorporar con prontitud el proceso de inducción a los funcionarios en la divulgación de las funciones y responsabilidades frente a la Seguridad de la Información seguridad de la información desde su vinculación, hasta su desvinculación.

- Revisar periódicamente el nivel de apropiación de la actualización del manual Modelo de Seguridad y Privacidad de la Información a funcionarios, contratistas y terceros, a través de métricas, con el fin de identificar la necesidad de reforzar las charlas, sesiones de trabajo, talleres y herramientas utilizadas.

- Identificar temas de interés afines con Seguridad de la Información, que lleven de primera mano a reconocer los estándares internacionales y buenas prácticas aplicables al instituto, en lo que refiere al nuevo y actualizado Manual de Políticas de Seguridad de la Información.

- El monitoreo de la efectividad de los nuevos controles de acceso lógico implantados para el Institutito Nacional de Vías. INVIAS, planta central, con el objeto de generar nuevas propuestas de mejora de acuerdo con las Políticas de Seguridad de la Información.

BIBLIOGRAFÍA

ALCALDÍA SANTIAGO DE CALI. Sistemas De Gestión y Control Integrados. Políticas de Seguridad de la Información. Disponible en: http://www.cali.gov.co/tic/publicaciones/1344/polticas_seguridad_de_la_informacin/

BY KENNETH C. Laudon, Jane Price Laudon, Sistemas de Información Gerencial, Administración de la empresa digital. Para minimizar errores, desastres, interrupciones de servicio, delitos por computadora y violaciones a la seguridad, se deben incorporar políticas y procedimientos especiales en el diseño e implementación de Sistemas de Información. Bogotá 18 -11- 2017.

Darleyocampo@yahoo.com. Universidad Piloto de Colombia. Modelo de Seguridad de la Información, para las Entidades Públicas del Estado Colombiano. Disponible en: http://polux.unipiloto.edu.co:8080/00002024.pdf

INSTITUTITO TÉCNICO CENTRAL. Escuela Tecnológica. Manual de Políticas de Seguridad y Privacidad de la Información. ETITC.

FRANCISCO RODRÍGUEZ-Henríquez. Ciudad de México. Noviembre 2003. Trabajo para obtener el grado de Maestra en Ciencias, en la especialidad de Ingeniería Electrónica.

FRONT COVER, Jesús Costas Santos. Mantenimiento de la seguridad en sistemas informáticos (MF0959_2), Starbook Editorial, S.A., La presente obra está dirigida a los estudiantes de los nuevos Certificados de Profesionalidad de la familia profesional Informática y Comunicaciones, en concreto al Módulo Formativo Mantenimiento de la Seguridad en Sistemas Informáticos.

GONZÁLEZ, Agudelo. Daniel Felipe. El Riesgo y la Falta de Políticas de Seguridad Informática, una amenaza en las empresas certificadas. 2014. Ensayo opción de grado Cr. ® Luis Alfredo Cabrera Albornoz Profesor Tutor Ensayo.

ICETEX. Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior. Manual de Políticas de Seguridad de la Información. Octubre 2014. Bogotá 18 -11- 2017.

INSTITUTO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Norma NTCGP 1000 y el estándar internacional, ISO 9001. Dentro del marco y del Decreto de fortalecimiento No. 2618 del 20 -11- 2013, Invias.Bogotá.2017.

INSTITUTO NACIONAL DE VIAS. INVIAS. Manual de Calidad y Gestión Integral del Instituto Nacional de Vías. INVIAS.

MIN TICS, Ministerio de Tecnologías de la Información y las Comunicaciones. Guía Metodológica de Pruebas de Efectividad, Instrumento de Evaluación MSPI. 18 -11- 2017.

MIN TICS, Ministerio de Tecnologías de la Información y las Comunicaciones. Controles de Seguridad y Privacidad de la Información. Guía No. 8. Bogotá 18 -11-2017

MIN TICS, Ministerio de Tecnologías de la Información y las Comunicaciones. Guía de Indicadores de Gestión para la Investigación de la Información. Guía No. 9. Bogotá 18-11-2017.

MINISTERIO DE TRANSPORTE. Decreto No. 2618 del 20 de noviembre de 2013 D.O. 48.980, del 20-11-2013.

MIN TICS, Ministerio de Tecnologías de la Información y las Comunicaciones. Subdirección de Estándares y Arquitectura TI, estándares modernos del manejo de la Información. Bogotá 18-11-2017.

M. en C. Abraham Jesús Basurto Becerra, " Aspectos de seguridad de Bitcon y su aplicación en una alternativa de infraestructura de llave pública ", Fecha de Grado: 17/12/2015, Director de Tesis: Dr. Francisco Rodríguez Henríquez.Mexico.2015.

M. en C. Abraham Jesús Basurto Becerra, " Aspectos de seguridad de Bitcon y su aplicación en una alternativa de infraestructura de llave pública ", Fecha de Grado: 17/12/2015, Director de Tesis: Dr. Francisco Rodríguez Henríquez.Mexico.2015.

M. en C. Laura Itzelt Reyes Montiel, "Estudio, Diseño y Evaluación de Protocolos de Autenticación para Redes Inalámbricas", CINVESTAV, enero 2004. Supervisor: Dr.

OWASP. Open Web Application Security Project. Estándar de Verificación de Seguridad en Aplicaciones 3.0.1. Bogotá 18 -11- 2017.

PRESIDENCIA DE LA REPUBLICA. Manual de Políticas de Seguridad de la Información.

UNESCO. Las Tecnologías de la Información y la Comunicación en la formación Docente. Guía de planificación. Coordinador: Evgueni Khvilon. 2004. Bogotá 18-11-2017

Dada su disposición a la mejora, El Invias evidencia los procesos administrativos, al convertirse en una bodega de información digital y es aquí donde se establece el trabajo de Seguridad de la Información

Tesis:

ALCALDÍA SANTIAGO DE CALI. Sistemas De Gestión y Control Integrados. Políticas de Seguridad de la Información. Disponible en: Link. http://www.cali.gov.co/tic/publicaciones/1344/polticas_seguridad_de_la_informacin/

BURGOS Salazar. Jorge, Pedro G. Campos. Modelo para la Seguridad de la Información. Universidad del Bío-Bío, Avenida Collao No. 1202, casilla 5-C P: 4081112, Concepción. Chile. Trabajo modelo para facilitar la obtención de un adecuado nivel de control de riesgo en Tecnologías de Información la Comunicación (TIC).

BY. Areitio J, Javier Areitio Bertolín. Seguridad de la Información. Redes informática y Sistemas de Información. Disponible en Link: https://books.google.com.co/books?id=_z2GcBD3deYC&printsec=frontcover&hl=es#v=onepage&q&f=false

Darleyocampo@yahoo.com. Universidad Piloto de Colombia. Modelo de Seguridad de la Información para entidades públicas del Estado Colombiano. Disponible en link: http://polux.unipiloto.edu.co:8080/00002024.pdf

ENISA. Beneficios, Riesgos y Recomendaciones para la Seguridad de la Información. Disponible en Link: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish

Ernst & Young Global. Seguridad de la información en un mundo sin fronteras. Disponible en Link: http://www.ey.com/Publication/vwLUAssets/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras/$FILE/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras.pdf

INSTITUTITO TÉCNICO CENTRAL. Escuela Tecnológica. Manual de Políticas de Seguridad y Privacidad de la Información. ETITC. Disponible en link: http://www.itc.edu.co/archives/manualpiliticassi.pdf

GONZÁLEZ, Agudelo. Daniel Felipe. El Riesgo y la falta de Políticas de Seguridad Informática, una amenaza en las empresas certificadas. 2014. Ensayo opción de grado Cr. ® Luis Alfredo Cabrera Albornoz Profesor Tutor Ensayo. Bogotá 2014.

ICETEX. Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior. Manual de Políticas de Seguridad de la Información. Octubre 2014.

ICONTEC. Norma Técnica NTC-ISO/IEC Colombiana 27001. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI), requisitos.

INSTITUTO NACIONAL DE VIAS-INVIAS. Manual de Calidad y Gestión Integral del Instituto Nacional de Vías. INVIAS. Disponible en Link: https://www.invias.gov.co/index.php/archivo-y-documentos/informacion-institucional/sistema-de-gestion-de-calidad/3884-manual-de-calidad-y-gestion-integral/file

Líneas de Investigación. Universidad Nacional Abierta y a Distancia Unad. Disponible en link: https://academia.unad.edu.co/images/escuelas/ecbti/Investigaci%C3%B3n/Grupos_por_cadena_de_formaci%C3%B3n/Cadena_de_formaci%C3%B3n_ETR.pdf

M. en C. Abraham Jesús Basurto Becerra, " Aspectos de seguridad de Bitcon y su aplicación en una alternativa de infraestructura de llave pública ", Fecha de Grado: 17/12/2015, Director de Tesis: Dr. Francisco Rodríguez Henríquez.Mexico.2015.

M. en C. Laura Itzelt Reyes Montiel, "Estudio, Diseño y Evaluación de Protocolos de Autenticación para Redes Inalámbricas", CINVESTAV, enero 2004. Supervisor: Dr. Francisco Rodríguez-Henríquez. Ciudad de México. Noviembre 2003. Trabajo Para obtener el grado de Maestra en Ciencias En la especialidad de Ingeniería Electrónica.

MIN TIC. Modelo de Seguridad. Fortalecimiento de la gestión TI en el Estado.

PRESIDENCIA DE LA REPUBLICA. Manual de Políticas de Seguridad de la Información. Disponible en link: http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/M-TI-01-Manual-Politicas-Seguridad-Informacion.pdf

PERAFÁN Ruiz. John Jairo. MILDRED Caicedo Cuchimba. Análisis de Riegos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor del Cauca.

Revista Tecnológica ESPOL – RTE., Vol.28, N 5, 492-507, (diciembre 2015). Metodología del Análisis y Evaluación del Riesgo, aplicados a la seguridad informática y de la información, bajo la Norma ISO/IEC 27001.

ROA, B. J. F. (2013). Seguridad informática. Madrid, ES: McGraw-Hill España. 2014

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS. Política para la Seguridad de la Información de la Universidad Francisco José de Caldas. Disponible en link: https://portalws.udistrital.edu.co/CIT/documentos/NORMATIVIDAD/politica_seguridad/archivos/Politica_para_Seguridad_Informacion_Version_0.0.1.0.pdf

UNIVERSIDAD CATÓLICA DE COLOMBIA. Diagnóstico y Actualización del Sistema de Gestión de Seguridad de la Información (SGSI), para ventas y servicios S.A. Bogota.2012.

UOC. Revista de los Estudios de Derecho y Ciencia Política de la UOC. El concepto de net neutrality y la tensión entre regulación pública y autorregulación privada de las redes.feb.2012.

LISTA DE ANEXOS

Anexo A. Activos Informáticos Del Instituto Nacional De Vías- INVIAS.

SERVICIO	DESCRIPCIÓN	ELEMENTO
SISTEMAS DE INFORMACIÓN	Corresponde a los aplicativos desarrollados internamente o por medio de contrato con terceros. Estos aplicativos modelan un proceso a través de funcionalidades automatizadas, con el fin de optimizar tiempos, generar una fuente única de información, fomentar el trabajo colaborativo, evitar reproceso innecesarios, integrar procesos, etc.	SEPRO-Seguimiento a proyectos de Inversión, para reportar a SPI-DNP. SIPLAN: Sistema de Planeación Institucional y evaluación desempeño. SITIO INTERNET E INTRANET. SYSTEM CENTER: Mesa de ayuda de servicios tecnológicos. SPI: Seguimiento Proyectos de Inversión (DNP). SUIFP: Sistema Unificado de Inversiones y Finanzas Públicas (DNP). SINERGIA: Seguimiento metas de Gobierno (DNP). PROJECT ONLINE: Seguimiento a proyectos Infraestructura sector transporte (Min transporté). SIG- Sistema de Información Geográfico. SIMA- Sistema de Información Ambiental. CIFRA- Sistema de Información para el seguimiento de contratos de obra. INVITRAMITES: trámite permisos para cierre de vías, uso de zona de carreteras y transporte de carga extra pesada y/o extra dimensionada VIAJERO SEGURO: Portal para consulta de eventos en la vía MAPA DE CARRETERAS: Portal para consulta de la red vial. RECVALOR: Aplicativo para el recaudo de valorización KACTUS-Sistema de Información Gestión Talento Humano (Nómina) SAI y SAE-Sistemas de Información de Inventarios (devolutivos y consumo) SIPRO-Sistema de Información Procesos Judiciales.

Fuente: Instituto Nacional de Vías-INVIAS.

Anexo A. (continuación)

SERVICIO	DESCRIPCIÓN	ELEMENTO
SISTEMAS DE INFORMACIÓN		SICO: Sistema de Información de contratos EMBARGOS: Aplicativo para control de embargos SIIF NACIÓN: Sistema de Información Financiero (Min hacienda)TRANSPARENCIA CONTRATACIÓN: Portal para publicación de procesos de contratación y manifestación de interés EQUAL: Portal para seguimiento preguntas, quejas, reclamos y sugerencias del ciudadano. SICOR: Sistema de Información de Correspondencia. WINISIS: Aplicativo para el control del archivo físico documental CXP: Aplicativo para control de cuentas por pagar PATI: Sistema de Gestión Documental (próximo a poner en marcha) DISCIPLINARIO: Aplicativo para control de procesos disciplinarios SILOG: Aplicativo para el control de la logística de vehículos. PORTAL DE COLOMBIA COMPRA: SECOP I, SECOP II y Tienda Virtual del Estado Colombiano. (Colombia Compra Eficiente) TRIBUTARIA: Aplicativo Gestión Tributaría DIGITURNO: Aplicativo para atención al ciudadano y carteleras electrónicas. SIRECI: Aplicativo para el reporte de la contratación a la CGR. (CGR) KAWAK- Aplicativo para el Sistema Integrado de Gestión Institucional.

Fuente: Instituto Nacional de Vías-INVIAS.

Anexo B. Categorías De Los Activos Las Vulnerabilidades, Amenazas De Seguridad Encontrados En el INVIAS.

Matriz de Análisis de Riesgo

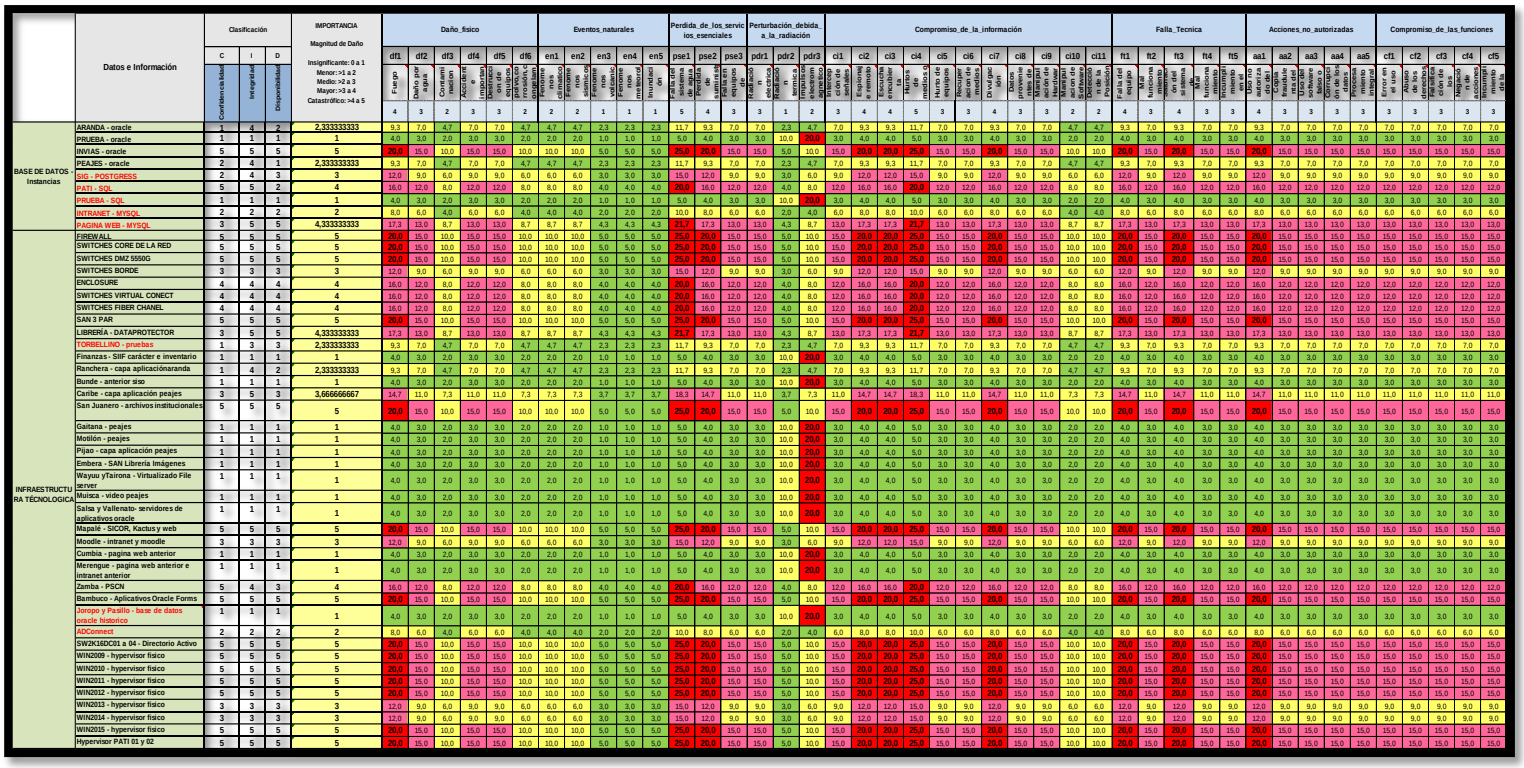
PROBABILIDAD
1 EXCEPCIONALMENTE : Puede ocurrir únicamente en circunstancias excepcionales
2 OCASIONALMENTE: Pudo ocurrir en algún momento
3 REGULARMENTE: Podría ocurrir en algún momento
4 GENERALMENTE: Probablemente ocurriría en la mayoría de las circunstancias
5 SIEMPRE: Se espera que ocurra en la mayoría de las circunstancias

	Datos e Información	Clasificación			IMPORTANCIA Magnitud de Daño Insignificante: 0 a 1 Menor: >1 a 2 Medio: >2 a 3 Mayor: >3 a 4 Catastrófico: >4 a 5	Daño_fisico						Eventos_naturales					Perdida_de_los_servicios_esenciales			Perturbación_debida_a_la_radiación			Compromiso_de_la_información											Falla_Tecnica					Acciones_no_autorizadas					Compromiso_de_las_funciones				
		C	I	D		df1	df2	df3	df4	df5	df6	en1	en2	en3	en4	en5	pse1	pse2	pse3	pdr1	pdr2	pdr3	ci1	ci2	ci3	ci4	ci5	ci6	ci7	ci8	ci9	ci10	ci11	ft1	ft2	ft3	ft4	ft5	aa1	aa2	aa3	aa4	aa5	cf1	cf2	cf3	cf4	cf5
		Confidencialidad	Integridad	Disponibilidad		Fuego	Daño por agua	Contaminacion	Accidente importante	Destruccion de equipos o	polvo,corrosión,congelamient	Fenomenos climatico	Fenomenos sismicos	Fenomenos volcanico	Fenomenos meteorolo	Inundación	Falla del sistema de agua o	Perdida de suministr	Falla en equipos de	Radiación electrica	Radiación termica	Impulsos electromagneticos	Intercepción de señales	Espionaje remoto	Escucha encubierta	Hurtos de medios o document	Hurto de equipos	Recuperacion de medios	Divulgación	Datos provenientes de	Manipulación de Hardware	Manipulacion de Software	Detección de la Posición	Falla del equipo	Mal funcionamiento	Saturación del sistema de	Mal funcionamiento	Incumplimiento en el	Uso no autorizado del	Copia fraudulenta del	Uso del software falso o	Corrupción de los datos	Procesamiento integral	Error en el uso	Abuso de los derechos	Falsificación de los derechos	Negación de acciones	Incumplimiento de la
						4	3	2	3	3	2	2	2	1	1	1	5	4	3	3	1	2	3	4	4	5	3	3	4	3	3	2	2	4	3	4	3	3	4	3	3	3	3	3	3	3	3	3
SOFTWARE	MOODLE	1	2	1	1,333333333	5,3	4,0	2,7	4,0	4,0	2,7	2,7	2,7	1,3	1,3	1,3	6,7	5,3	4,0	4,0	1,3	2,7	4,0	5,3	5,3	5,7	4,0	4,0	5,3	4,0	4,0	2,7	2,7	5,3	4,0	5,3	4,0	4,0	5,3	4,0	4,0	4,0	4,0	4,0	4,0	4,0	4,0	4,0
	SIRI	1	2	2	1,666666667	6,7	5,0	3,3	5,0	5,0	3,3	3,3	3,3	1,7	1,7	1,7	8,3	6,7	5,0	5,0	1,7	3,3	5,0	6,7	6,7	8,3	5,0	5,0	6,7	5,0	5,0	3,3	3,3	6,7	5,0	6,7	5,0	5,0	6,7	5,0	5,0	5,0	5,0	5,0	5,0	5,0	5,0	5,0
	SILOG	1	2	1	1,333333333	5,3	4,0	2,7	4,0	4,0	2,7	2,7	2,7	1,3	1,3	1,3	6,7	5,3	4,0	4,0	1,3	2,7	4,0	5,3	5,3	6,7	4,0	4,0	5,3	4,0	4,0	2,7	2,7	5,3	4,0	5,3	4,0	4,0	5,3	4,0	4,0	4,0	4,0	4,0	4,0	4,0	4,0	4,0
	SAE	1	3	2	2	8,0	6,0	4,0	6,0	6,0	4,0	4,0	4,0	2,0	2,0	2,0	10,0	8,0	6,0	6,0	2,0	4,0	6,0	8,0	8,0	10,0	6,0	6,0	8,0	6,0	6,0	4,0	4,0	8,0	6,0	8,0	6,0	6,0	8,0	6,0	6,0	6,0	6,0	6,0	6,0	6,0	6,0	6,0
	INTRANET	1	2	3	2	8,0	6,0	4,0	6,0	6,0	4,0	4,0	4,0	2,0	2,0	2,0	10,0	8,0	6,0	6,0	2,0	4,0	6,0	8,0	8,0	10,0	6,0	6,0	8,0	6,0	6,0	4,0	4,0	8,0	6,0	8,0	6,0	6,0	8,0	6,0	6,0	6,0	6,0	6,0	6,0	6,0	6,0	6,0
	SIPLAN	1	4	2	2,333333333	9,3	7,0	4,7	7,0	7,0	4,7	4,7	4,7	2,3	2,3	2,3	11,7	9,3	7,0	7,0	2,3	4,7	7,0	9,3	9,3	11,7	7,0	7,0	9,3	7,0	7,0	4,7	4,7	9,3	7,0	9,3	7,0	7,0	9,3	7,0	7,0	7,0	7,0	7,0	7,0	7,0	7,0	7,0
	SAI	1	4	2	2,333333333	9,3	7,0	4,7	7,0	7,0	4,7	4,7	4,7	2,3	2,3	2,3	11,7	9,3	7,0	7,0	2,3	4,7	7,0	9,3	9,3	11,7	7,0	7,0	9,3	7,0	7,0	4,7	4,7	9,3	7,0	9,3	7,0	7,0	9,3	7,0	7,0	7,0	7,0	7,0	7,0	7,0	7,0	7,0
	SIPRO	2	3	2	2,333333333	9,3	7,0	4,7	7,0	7,0	4,7	4,7	4,7	2,3	2,3	2,3	11,7	9,3	7,0	7,0	2,3	4,7	7,0	9,3	9,3	11,7	7,0	7,0	9,3	7,0	7,0	4,7	4,7	9,3	7,0	9,3	7,0	7,0	9,3	7,0	7,0	7,0	7,0	7,0	7,0	7,0	7,0	7,0
	KAWAK	1	3	3	2,333333333	9,3	7,0	4,7	7,0	7,0	4,7	4,7	4,7	2,3	2,3	2,3	11,7	9,3	7,0	7,0	2,3	4,7	7,0	9,3	9,3	11,7	7,0	7,0	9,3	7,0	7,0	4,7	4,7	9,3	7,0	9,3	7,0	7,0	9,3	7,0	7,0	7,0	7,0	7,0	7,0	7,0	7,0	7,0
	VIAJERO SEGURO	1	4	5	3,333333333	13,3	10,0	6,7	10,0	10,0	6,7	6,7	6,7	3,3	3,3	3,3	16,7	13,3	10,0	10,0	3,3	6,7	10,0	13,3	13,3	16,7	10,0	10,0	13,3	10,0	10,0	6,7	6,7	13,3	10,0	13,3	10,0	10,0	13,3	10,0	10,0	10,0	10,0	10,0	10,0	10,0	10,0	10,0
	SIREV - VALORIZACION	1	4	2	2,333333333	9,3	7,0	4,7	7,0	7,0	4,7	4,7	4,7	2,3	2,3	2,3	11,7	9,3	7,0	7,0	2,3	4,7	7,0	9,3	9,3	11,7	7,0	7,0	9,3	7,0	7,0	4,7	4,7	9,3	7,0	9,3	7,0	7,0	9,3	7,0	7,0	7,0	7,0	7,0	7,0	7,0	7,0	7,0
	INVITRAMITES	3	5	5	4,333333333	17,3	13,0	8,7	13,0	13,0	8,7	8,7	8,7	4,3	4,3	4,3	21,7	17,3	13,0	13,0	4,3	8,7	13,0	17,3	17,3	21,7	13,0	13,0	17,3	13,0	13,0	8,7	8,7	17,3	13,0	17,3	13,0	13,0	17,3	13,0	13,0	13,0	13,0	13,0	13,0	13,0	13,0	13,0
	EQUAL QRS	4	3	3	3,333333333	13,3	10,0	6,7	10,0	10,0	6,7	6,7	6,7	3,3	3,3	3,3	16,7	13,3	10,0	10,0	3,3	6,7	10,0	13,3	13,3	16,7	10,0	10,0	13,3	10,0	10,0	6,7	6,7	13,3	10,0	13,3	10,0	10,0	13,3	10,0	10,0	10,0	10,0	10,0	10,0	10,0	10,0	10,0
	SIIF GRAFICO	3	4	2	3	12,0	9,0	6,0	9,0	9,0	6,0	6,0	6,0	3,0	3,0	3,0	15,0	12,0	9,0	9,0	3,0	6,0	9,0	12,0	12,0	15,0	9,0	9,0	12,0	9,0	9,0	6,0	6,0	12,0	9,0	12,0	9,0	9,0	12,0	9,0	9,0	9,0	9,0	9,0	9,0	9,0	9,0	9,0
	SIEV – EVASION PEAJES	2	5	2	3	12,0	9,0	6,0	9,0	9,0	6,0	6,0	6,0	3,0	3,0	3,0	15,0	12,0	9,0	9,0	3,0	6,0	9,0	12,0	12,0	15,0	9,0	9,0	12,0	9,0	9,0	6,0	6,0	12,0	9,0	12,0	9,0	9,0	12,0	9,0	9,0	9,0	9,0	9,0	9,0	9,0	9,0	9,0
	SICOR	2	5	4	3,666666667	14,7	11,0	7,3	11,0	11,0	7,3	7,3	7,3	3,7	3,7	3,7	18,3	14,7	11,0	11,0	3,7	7,3	11,0	14,7	14,7	18,3	11,0	11,0	14,7	11,0	11,0	7,3	7,3	14,7	11,0	14,7	11,0	11,0	14,7	11,0	11,0	11,0	11,0	11,0	11,0	11,0	11,0	11,0
	SICO	2	5	4	3,666666667	14,7	11,0	7,3	11,0	11,0	7,3	7,3	7,3	3,7	3,7	3,7	18,3	14,7	11,0	11,0	3,7	7,3	11,0	14,7	14,7	18,3	11,0	11,0	14,7	11,0	11,0	7,3	7,3	14,7	11,0	14,7	11,0	11,0	14,7	11,0	11,0	11,0	11,0	11,0	11,0	11,0	11,0	11,0
	PAGINA WEB	1	5	5	3,666666667	14,7	11,0	7,3	11,0	11,0	7,3	7,3	7,3	3,7	3,7	3,7	18,3	14,7	11,0	11,0	3,7	7,3	11,0	14,7	14,7	18,3	11,0	11,0	14,7	11,0	11,0	7,3	7,3	14,7	11,0	14,7	11,0	11,0	14,7	11,0	11,0	11,0	11,0	11,0	11,0	11,0	11,0	11,0
	KACTUS	2	5	4	3,666666667	14,7	11,0	7,3	11,0	11,0	7,3	7,3	7,3	3,7	3,7	3,7	18,3	14,7	11,0	11,0	3,7	7,3	11,0	14,7	14,7	18,3	11,0	11,0	14,7	11,0	11,0	7,3	7,3	14,7	11,0	14,7	11,0	11,0	14,7	11,0	11,0	11,0	11,0	11,0	11,0	11,0	11,0	11,0
	RECAUDO Y CONTROL PEAJES	2	5	1	2,666666667	10,7	8,0	5,3	8,0	8,0	5,3	5,3	5,3	2,7	2,7	2,7	13,3	10,7	8,0	8,0	2,7	5,3	8,0	10,7	10,7	13,3	8,0	8,0	10,7	8,0	8,0	5,3	5,3	10,7	8,0	10,7	8,0	8,0	10,7	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0
	SIG	2	5	1	2,666666667	10,7	8,0	5,3	8,0	8,0	5,3	5,3	5,3	2,7	2,7	2,7	13,3	10,7	8,0	8,0	2,7	5,3	8,0	10,7	10,7	13,3	8,0	8,0	10,7	8,0	8,0	5,3	5,3	10,7	8,0	10,7	8,0	8,0	10,7	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0
	CIFRA	2	5	3	3,333333333	13,3	10,0	6,7	10,0	10,0	6,7	6,7	6,7	3,3	3,3	3,3	16,7	13,3	10,0	10,0	3,3	6,7	10,0	13,3	13,3	16,7	10,0	10,0	13,3	10,0	10,0	6,7	6,7	13,3	10,0	13,3	10,0	10,0	13,3	10,0	10,0	10,0	10,0	10,0	10,0	10,0	10,0	10,0
	EMBARGOS	2	5	1	2,666666667	10,7	8,0	5,3	8,0	8,0	5,3	5,3	5,3	2,7	2,7	2,7	13,3	10,7	8,0	8,0	2,7	5,3	8,0	10,7	10,7	13,3	8,0	8,0	10,7	8,0	8,0	5,3	5,3	10,7	8,0	10,7	8,0	8,0	10,7	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0
	SISO	1	5	5	3,666666667	14,7	11,0	7,3	11,0	11,0	7,3	7,3	7,3	3,7	3,7	3,7	18,3	14,7	11,0	11,0	3,7	7,3	11,0	14,7	14,7	18,3	11,0	11,0	14,7	11,0	11,0	7,3	7,3	14,7	11,0	14,7	11,0	11,0	14,7	11,0	11,0	11,0	11,0	11,0	11,0	11,0	11,0	11,0
	WINISIS	2	5	1	2,666666667	10,7	8,0	5,3	8,0	8,0	5,3	5,3	5,3	2,7	2,7	2,7	13,3	10,7	8,0	8,0	2,7	5,3	8,0	10,7	10,7	13,3	8,0	8,0	10,7	8,0	8,0	5,3	5,3	10,7	8,0	10,7	8,0	8,0	10,7	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0
	PATI	4	4	1	3	12,0	9,0	6,0	9,0	9,0	6,0	6,0	6,0	3,0	3,0	3,0	15,0	12,0	9,0	9,0	3,0	6,0	9,0	12,0	12,0	15,0	9,0	9,0	12,0	9,0	9,0	6,0	6,0	12,0	9,0	12,0	9,0	9,0	12,0	9,0	9,0	9,0	9,0	9,0	9,0	9,0	9,0	9,0
	PROCESOS CONTROL DISCIPLINARIO INTERNO	4	5	1	3,333333333	13,3	10,0	6,7	10,0	10,0	6,7	6,7	6,7	3,3	3,3	3,3	16,7	13,3	10,0	10,0	3,3	6,7	10,0	13,3	13,3	16,7	10,0	10,0	13,3	10,0	10,0	6,7	6,7	13,3	10,0	13,3	10,0	10,0	13,3	10,0	10,0	10,0	10,0	10,0	10,0	10,0	10,0	10,0
	DIGITURNO	1	2	1	1,333333333	5,3	4,0	2,7	4,0	4,0	2,7	2,7	2,7	1,3	1,3	1,3	6,7	5,3	4,0	4,0	1,3	2,7	4,0	5,3	5,3	5,7	4,0	4,0	5,3	4,0	4,0	2,7	2,7	5,3	4,0	5,3	4,0	4,0	5,3	4,0	4,0	4,0	4,0	4,0	4,0	4,0	4,0	4,0
	SEPRO	2	5	2	3	12,0	9,0	6,0	9,0	9,0	6,0	6,0	6,0	3,0	3,0	3,0	15,0	12,0	9,0	9,0	3,0	6,0	9,0	12,0	12,0	15,0	9,0	9,0	12,0	9,0	9,0	6,0	6,0	12,0	9,0	12,0	9,0	9,0	12,0	9,0	9,0	9,0	9,0	9,0	9,0	9,0	9,0	9,0
	GESTION TRIBUTARIA	2	5	1	2,666666667	10,7	8,0	5,3	8,0	8,0	5,3	5,3	5,3	2,7	2,7	2,7	13,3	10,7	8,0	8,0	2,7	5,3	8,0	10,7	10,7	13,3	8,0	8,0	10,7	8,0	8,0	5,3	5,3	10,7	8,0	10,7	8,0	8,0	10,7	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0	8,0
	CONTROL DE ACCESO	2	5	4	3,666666667	14,7	11,0	7,3	11,0	11,0	7,3	7,3	7,3	3,7	3,7	3,7	18,3	14,7	11,0	11,0	3,7	7,3	11,0	14,7	14,7	18,3	11,0	11,0	14,7	11,0	11,0	7,3	7,3	14,7	11,0	14,7	11,0	11,0	14,7	11,0	11,0	11,0	11,0	11,0	11,0	11,0	11,0	11,0
	Aplicativo LECTURAS AMBIENTALES	1	5	1	2,333333333	9,3	7,0	4,7	7,0	7,0	4,7	4,7	4,7	2,3	2,3	2,3	11,7	9,3	7,0	7,0	2,3	4,7	7,0	9,3	9,3	11,7	7,0	7,0	9,3	7,0	7,0	4,7	4,7	9,3	7,0	9,3	7,0	7,0	9,3	7,0	7,0	7,0	7,0	7,0	7,0	7,0	7,0	7,0
	DATAPROTECTOR	1	5	1	2,333333333	9,3	7,0	4,7	7,0	7,0	4,7	4,7	4,7	2,3	2,3	2,3	11,7	9,3	7,0	7,0	2,3	4,7	7,0	9,3	9,3	11,7	7,0	7,0	9,3	7,0	7,0	4,7	4,7	9,3	7,0	9,3	7,0	7,0	9,3	7,0	7,0	7,0	7,0	7,0	7,0	7,0	7,0	7,0
	SYSTEM CENTER	1	5	3	3	12,0	9,0	6,0	9,0	9,0	6,0	6,0	6,0	3,0	3,0	3,0	15,0	12,0	9,0	9,0	3,0	6,0	9,0	12,0	12,0	15,0	9,0	9,0	12,0	9,0	9,0	6,0	6,0	12,0	9,0	12,0	9,0	9,0	12,0	9,0	9,0	9,0	9,0	9,0	9,0	9,0	9,0	9,0
	Gestión de Proyectos de Infraestructura -GPI	1	5	1	2,333333333	9,3	7,0	4,7	7,0	7,0	4,7	4,7	4,7	2,3	2,3	2,3	11,7	9,3	7,0	7,0	2,3	4,7	7,0	9,3	9,3	11,7	7,0	7,0	9,3	7,0	7,0	4,7	4,7	9,3	7,0	9,3	7,0	7,0	9,3	7,0	7,0	7,0	7,0	7,0	7,0	7,0	7,0	7,0
	ACROBAT PRO - ESCRITORIO	1	2	1	1,333333333	5,3	4,0	2,7	4,0	4,0	2,7	2,7	2,7	1,3	1,3	1,3	6,7	5,3	4,0	4,0	1,3	2,7	4,0	5,3	5,3	5,7	4,0	4,0	5,3	4,0	4,0	2,7	2,7	5,3	4,0	5,3	4,0	4,0	5,3	4,0	4,0	4,0	4,0	4,0	4,0	4,0	4,0	4,0
	PCSECURE	1	2	1	1,333333333	5,3	4,0	2,7	4,0	4,0	2,7	2,7	2,7	1,3	1,3	1,3	6,7	5,3	4,0	4,0	1,3	2,7	4,0	5,3	5,3	5,7	4,0	4,0	5,3	4,0	4,0	2,7	2,7	5,3	4,0	5,3	4,0	4,0	5,3	4,0	4,0	4,0	4,0	4,0	4,0	4,0	4,0	4,0
	SISTEMAS OPERATIVOS - servidores	5	5	5	5	20,0	15,0	10,0	15,0	15,0	10,0	10,0	10,0	5,0	5,0	5,0	25,0	20,0	15,0	15,0	5,0	10,0	15,0	20,0	20,0	25,0	15,0	15,0	20,0	15,0	15,0	10,0	10,0	20,0	15,0	20,0	15,0	15,0	20,0	15,0	15,0	15,0	15,0	15,0	15,0	15,0	15,0	15,0
	SISTEMAS OPERATIVOS - cliente final	3	5	1	3	12,0	9,0	6,0	9,0	9,0	6,0	6,0	6,0	3,0	3,0	3,0	15,0	12,0	9,0	9,0	3,0	6,0	9,0	12,0	12,0	15,0	9,0	9,0	12,0	9,0	9,0	6,0	6,0	12,0	9,0	12,0	9,0	9,0	12,0	9,0	9,0	9,0	9,0	9,0	9,0	9,0	9,0	9,0
	MS-OFFICE	3	5	1	3	12,0	9,0	6,0	9,0	9,0	6,0	6,0	6,0	3,0	3,0	3,0	15,0	12,0	9,0	9,0	3,0	6,0	9,0	12,0	12,0	15,0	9,0	9,0	12,0	9,0	9,0	6,0	6,0	12,0	9,0	12,0	9,0	9,0	12,0	9,0	9,0	9,0	9,0	9,0	9,0	9,0	9,0	9,0

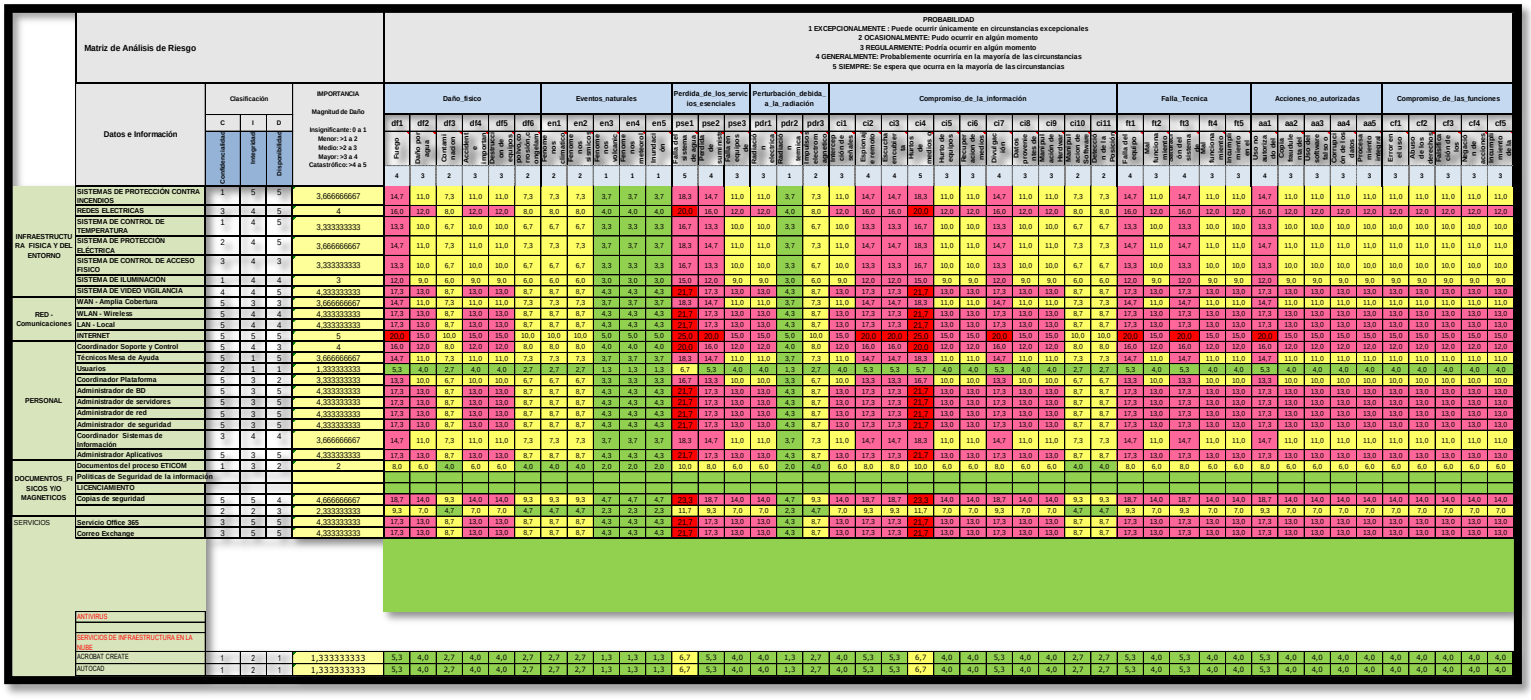
Fuente: Instituto Nacional de Vías. INVIAS. Planta Central.[22]

[22] Actualización_Análisis Matriz Riesgo Consolidada.xls

Anexo B. (continuación)



Fuente: Instituto Nacional de Vías. INVIAS. Planta Central.
Link: Actualización Análisis Matriz Riesgo Consolidada.xls



Fuente: Instituto Nacional de Vías. INVIAS. Planta Central.
Link: Actualización Análisis Matriz Riesgo Consolidada.xls

Anexo C. Vulnerabilidades, Amenazas De Seguridad Encontrados En el Instituto Nacional de Vías- INVIAS- Nivel Planta Central.

TIPO	ACTIVO	VULNERABILIDADES	AMENAZAS	RIESGOS
D	Datos Sensibles Activo Informático de la Entidad- Planta Central. INVIAS	• Pérdida de información sensible para la entidad Instituto Nacional de Vías- Invias- Planta Central, por eliminación intencional. Circulación de información por medio de personas no autorizadas. • La información sea modificada sin autorización	• Pérdida de la Información. • Robo o divulgación no autorizada de información crítica o sensible. • Alteración o pérdida parcial de Información.	• Perdida Información • Perdida integridad datos. Instituto Nacional de Vias- Invias- Planta Central.
K	Claves Criptográficas	• Permitan el acceso a la información sensible de la organización. • Perdida Integridad de la información.	• Acceso a la información por personas no autorizadas	• Fuga de información
S	Servicios Informáticos Adicionales del Instituto Nacional de Vías. INVIAS, planta central	• Mala configuración planta telefónica. • Mala configuración del envió y recibo de correos institucionales. • Envió de información no autorizada a terceros. • Falta de concienciación en el uso del correo institucional.	• No se tenga la disponibilidad de la comunicación mediante voz. • Divulgación de información no autorizada. • Falla técnica al recibir o enviar correos electrónicos	• Fuga de información. • Acceso no autorizado a la información vital de la empresa INVIAS, por personas no autorizadas. • Incomunicación vía voz IP

Fuente: Autor.

Anexo C. (Continuación)

TIPO	ACTIVO	VULNERABILIDADES	AMENAZAS	RIESGOS
Media	Soporte de Información	• Descuido de los activos de información. Información no cifrada divulgada.	• Malware Desorden del funcionario uso	• Pérdida y falta de confiabilidad de la Información almacenada en un dispositivo.
SW	Redes de Comunicación Informática Entidad-Instituto Nacional de Vías-INVIAS Planta Central.	• Ausencia /fallas de planes de Contingencia • Ausencia de monitoreo sobre la red • Administración de red inadecuada • Herramientas de detección / prevención inexistentes o inadecuadas • Ubicación en sitios deficientes en seguridad física (sitios sin control de acceso adecuados) • Falta /falla de políticas para el trabajo en áreas seguras • Condiciones de instalaciones, mantenimiento y operación inadecuadas.	• Uso inadecuado/no autorizado del recurso. • Daños Accidentales. • Falla del medio de comunicación. • Pérdida de disponibilidad y/o disminución de la calidad del servicio. • Pérdida de la Información. • Robo o divulgación no autorizada de información crítica o sensible. • Alteración o pérdida parcial de la información.	• Pérdida de la Información almacenada en el servidor.
COM		• Inundación centro de cómputo. • Mal configuración de la energía. • Descarga eléctrica no controlada.	• Daño del hardware en el centro de cómputo. • Ataque informático. • Alteración o pérdida parcial de la información.	• Falla técnica en la red. • Destrucción de la información.

Fuente: Autor

Anexo C. (Continuación)

TIPO	ACTIVO	VULNERABILIDADES	AMENAZAS	RIESGOS
AUX	Equipamiento Auxiliar	• Desconocimiento de las normas técnicas en el uso de redes eléctricas.	• Falla técnica en el aire acondicionado ubicado en el centro de cómputo. • Obsolescencia en el inmobiliario. • Daño en la UPS.	• Perdida de la información almacenada en los Servidores en el centro de computo
L	Instalaciones	• Falta de mantenimiento de la infraestructura física del edificio. • Falta de seguridad a personas • No tener el protocolo de continuidad del negocio.	• Sismo • Inundación Acto Terrorista	• Perdida en disponibilidad de los Activos de Información.
P	Personal	• Perdida de independencia en el manejo de la Información vital de la empresa por personal de la entidad influenciada por otros. • Fallas en la incorporación del personal. • Compartimentación de la información por parte de funcionarios.	• Necesidades del funcionario, nivel monetario. • Inconformismo del funcionario. • Falta de entrenamiento de los procesos asignados	• Perdida en la confidencialidad de la Información vital. • Perdida en la integridad de la Información.

Fuente: Autor

Anexo D. Listas De Chequeo Para Verificación

Ítem	Controles	NM (%)
A.5..	POLÍTICA DE SEGURIDAD.	80%
A.5.1.	Política de Seguridad de la Información.	80%
A.5.1.1	Políticas para la Seguridad de la Información.	80%
A.5.1.2	Revisión de la política de seguridad de la información	80%
A.6..	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	80%
A.6.1.	Organización interna	80%
A.6.1.1	Seguridad de la información Roles y responsabilidades	80%
A.6.1.2	Separación de deberes	80%
A.6.1.3	Contacto con las autoridades	80%
A.6.1.4	Contacto con grupos de interés especial	80%
A.6.1.5	Seguridad de la información en gestión de proyectos	80%
A.6.2.	Dispositivos móviles y teletrabajo	80%
A.6.2.1	Política para dispositivos móviles	80%
A.6.2.2	Teletrabajo	80%
A.7..	SEGURIDAD DE LOS RECURSOS HUMANOS	80%
A.7.1.	Antes de asumir el empleo	80%
A.7.1.1	Selección	80%
A.7.1.2	Términos y condiciones del empleo	80%
A.7.2.	Durante la ejecución del empleo	80%
A.7.2.1	Responsabilidades de la dirección	80%
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	80%
A.7.2.3	Proceso disciplinario	80%
A.7.3.	Terminación y cambio de empleo	80%
A.7.3.1	Terminación o cambio de responsabilidades de empleo	80%
A.8..	GESTIÓN DE ACTIVOS	82%
A.8.1.	Responsabilidad por los activos	80%
A.8.1.1	Inventario de activos	80%
A.8.1.2	Propiedad de los activos	80%
A.8.1.3	Uso aceptable de los activos	80%
A.8.1.4	Devolución de activos	80%
A.8.2.	Clasificación de la información	87%
A.8.2.1	Clasificación de la información	100%
A.8.2.2	Etiquetado de la información	80%
A.8.2.3	Manejo de activos	80%
A.8.3.	Manejo de medios de soporte	80%

Fuente: Autor - Instituto Nacional de Vías. INVIAS.

Anexo D. (Continuación)

Ítem	Controles	NM (%)
A.8.3.1	Gestión de medios de soporte removibles	80%
A.8.3.2	Disposición de los medios de soporte	80%
A.8.3.3	Transferencia de medios de soporte físicos	80%
A.9..	CONTROL DE ACCESO	81%
A.9.1.1	Requisitos del negocio para control de acceso	90%
A.9.1.2	Política de control de acceso	80%
A.9.1.3	Acceso a redes y a servicios en red	100%
A.9.2.	Gestión de acceso de usuarios	80%
A.9.2.1	Registro y cancelación del registro de usuarios	80%
A.9.2.2	Suministro de acceso de usuarios	80%
A.9.2.3	Gestión de derechos de acceso privilegiado	80%
A.9.2.4	Gestión de información de autenticación secreta de usuarios	80%
A.9.2.5	Revisión de los derechos de acceso de usuarios	80%
A.9.2.6	Retiro o ajuste de los derechos de acceso	80%
A.9.3.	Responsabilidades de los usuarios	80%
A.9.3.1	Uso de información de autenticación secreta	80%
A.9.4.	Control de acceso a sistemas y aplicaciones	72%
A.9.4.1	Restricción de acceso a información	80%
A.9.4.2	Procedimiento de ingreso seguro	80%
A.9.4.3	Sistema de gestión de contraseñas	80%
A.9.4.4	Uso de programas utilitarios privilegiados	60%
A.9.4.5	Control de acceso a códigos fuente de programas	60%
A.10..	CRIPTOGRAFÍA	80%
A.10.1.	Controles criptográficos	80%
A.10.1.1	Política sobre el uso de controles criptográficos	80%
A.10.1.2	Gestión de claves	80%
A.11..	SEGURIDAD FÍSICA Y DEL ENTORNO	80%
A.11.1.	Áreas Seguras	80%
A.11.1.1	Perímetro de seguridad física	80%
A.11.1.2	Controles de acceso físico	80%
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	80%
A.11.1.4	Protección contra amenazas externas y ambientales	80%
A.11.1.5	Trabajo en áreas seguras	80%
A.11.1.6	Áreas de carga, despacho y acceso público	80%
A.11.2.	Equipos	80%
A.11.2.1	Ubicación y protección de los equipos	80%

Fuente: Autor - Instituto Nacional de Vías. INVIAS.

Anexo D. (Continuación)

Ítem	Controles	NM (%)
A.11.2.2	Servicios públicos de soporte	80%
A.11.2.3	Seguridad del cableado	80%
A.11.2.4	Mantenimiento de los equipos	80%
A.11.2.5	Retiro de activos	80%
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	80%
A.11.2.7	Disposición segura o reutilización de equipos	80%
A.11.2.8	Equipos de usuario desatendido	80%
A.11.2.9	Política de escritorio limpio y pantalla limpia	80%
A.12..	SEGURIDAD DE LAS OPERACIONES	79%
A.12.1.	Procedimientos Operacionales y Responsabilidades	75%
A.12.1.1	Documentación de los procedimientos de operación	80%
A.12.1.2	Gestión del cambios	80%
A.12.1.3	Gestión de la capacidad	60%
A.12.1.4	Separación de las instalaciones de desarrollo, pruebas y operación	80%
A.12.2.	Protección contra códigos maliciosos	80%
A.12.2.1	Controles contra códigos maliciosos.	80%
A.12.3.	Copias de respaldo	80%
A.12.3.1	Copias de respaldo de la información	80%
A.12.4.	Registro y seguimiento	80%
A.12.4.1	Registro de eventos	80%
A.12.4.2	Protección de la información de registro	80%
A.12.4.3	Registros del administrador y del operador	80%
A.12.4.4	Sincronización de relojes	80%
A.12.5.	Control de software operacional	80%
A.12.5.1	Instalación de software en sistemas operativos	80%
A.12.6.	Gestión de la vulnerabilidad técnica	80%
A.12.6.1	Gestión de las vulnerabilidades técnicas	80%
A.12.6.2	Restricciones sobre la instalación de software.	80%
A.12.7.	Consideraciones sobre auditorías de sistemas de información	80%
A.12.7.1	Controles de auditorías de sistemas de información.	80%
A.13..	SEGURIDAD DE LAS COMUNICACIONES	53%
A.13.1.	Gestión de la seguridad de redes	80%
A.13.1.1	Controles de redes	80%
A.13.1.2	Seguridad de los servicios de red.	80%
A.13.1.3	Separación en las redes	80%
A.13.2.	Transferencia de información	80%

Fuente: Autor - Instituto Nacional de Vías. INVIAS.

Anexo D. (Continuación)

Ítem	Controles	NM (%)
A.13.2.1	Políticas y procedimientos de transferencia de información	80%
A.13.2.2	Acuerdos sobre transferencia de información	80%
A.13.2.3	Mensajes electrónicos	80%
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	80%
A.14..	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	71%
A.14.1.	Requisitos de seguridad de los sistemas de información	73%
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	60%
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	80%
A.14.1.3	Protección de transacciones de servicios de aplicaciones	80%
A.14.2.	Seguridad en los procesos de desarrollo y de soporte	80%
A.14.2.1	Política de desarrollo seguro	80%
A.14.2.2	Procedimientos de control de cambios en sistemas	80%
A.14.2.3	Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	80%
A.14.2.4	Restricciones en los cambios a los paquetes de software	80%
A.14.2.5	Principios de construcción de los sistemas seguros	80%
A.14.2.6	Ambiente de desarrollo seguro	80%
A.14.2.7	Desarrollo contratado externamente	80%
A.14.2.8	Pruebas de seguridad de sistemas	80%
A.14.2.9	Prueba de aceptación de sistemas	80%
A.14.3.	Datos de prueba	60%
A.14.3.1	Protección de datos de prueba	60%
A.15..	RELACIONES CON LOS PROVEEDORES	80%
A.15.1.	Seguridad de la información en las relaciones con los proveedores	80%
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	80%
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	80%
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	80%
A.15.2.	Gestión de la prestación de servicios de proveedores	80%
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	80%
A.15.2.2	Gestión de cambios a los servicios de los proveedores	80%
A.16..	GESTIÓN DE INCIDENTES DE SEGURIDAD	80%
A.16.1.	Gestión de incidentes y mejoras en la seguridad de la información	80%
A.16.1.1	Responsabilidades y procedimientos	80%
A.16.1.2	Reporte de eventos de seguridad de la información	80%

Fuente: Autor - Instituto Nacional de Vías. INVIAS.

Anexo D. (Continuación)

Ítem	Controles	NM (%)
A.16.1.3	Reporte de debilidades de seguridad de la información	80%
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	80%
A.16.1.5	Respuesta a incidentes de seguridad de la información	80%
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	80%
A.16.1.7	Recolección de evidencia	80%
A.17..	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	80%
A.17.1.	Continuidad de seguridad de la información	80%
A.17.1.1	Planificación de la continuidad de la seguridad de la información	80%
A.17.1.2	Implementación de la continuidad de la seguridad de la información	80%
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	80%
A.17.2.	Redundancias	80%
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	80%
A.18..	CUMPLIMIENTO	80%
A.18.1.	Cumplimiento de requisitos legales y contractuales	80%
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	80%
A.18.1.2	Derechos de propiedad intelectual	80%
A.18.1.3	Protección de registros	80%
A.18.1.4	Privacidad y protección de información de datos personales	80%
A.18.1.5	Reglamentación de controles criptográficos	80%
A.18.2.	Revisiones de seguridad de la información	80%
A.18.2.1	Revisión independiente de la seguridad de la información	80%
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	80%
A.18.2.3	Revisión del cumplimiento técnico	80%
TOTAL	**78%**	

Fuente: Autor - Instituto Nacional de Vías. INVIAS.

Título de Documento.	ESTUDIO Y DIAGNOSTICO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, PARA EL INSTITUTO NACIONAL DE VIAS. INVIAS-PLANTA CENTRAL
Autor	MARIBEL CRUZ ARGUELLO
Palabras Claves	Dato, Control, Información, Rol, Sistema de información, Vulnerabilidad, Seguridad, integridad, disponibilidad, confidencialidad, autenticidad, Activo informático, redes.

CONTENIDO:

EL DIAGNOSTICO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL INSTITUTO NACIONAL DE VIAS. INVIAS, PLANTA CENTRAL.

- **DESCRIPCIÓN DEL PROBLEMA:**

Los servicios tecnológicos, información y de Comunicación en el Instituto Nacional de Vías INVIAS, se ofrecen gracias a la infraestructura técnica, tecnológica y de seguridad de la información, con la que se cuenta la entidad.

A su vez el Estado Colombiano diseñó la estrategia Gobierno En Línea – GEL, la cual establece los lineamientos de la gestión de TI en el sector Gobierno, recogiendo estándares mundiales y mejores prácticas de gobierno electrónico y de buen uso de la tecnología como herramienta de publicidad y transparencia.

Para lograr lo anteriormente establecido, se plantea como herramienta transversal el Marco de Referencia de Arquitectura Empresarial, que orienta sobre mejores prácticas, guías y estándares en el uso adecuado de la tecnología como soporte de procesos y servicios, hacia la consecución y logro de la Misión de la entidad.

En cumplimiento de la Estrategia GEL y acorde con el desarrollo Tecnológico, en INVIAS se ofrecen los servicios tecnológicos, agrupados según el beneficio general que se reciben y perciben los usuarios, para que sean de mejor entendimiento, así:

- Servicios de ofimática
- Servicios de conectividad/comunicaciones
- Sistemas de información
- Soporte técnico
- Servicios seguridad de la información.

Recursos tecnológicos que el Instituto Nacional de Vías. INVIAS, planta central, pone a disposición de trabajadores, Contratistas y ciudadanos, para proveer y optimizar el trabajo y la consulta de sus aplicaciones.

OBJETIVO GENERAL.

Analizar el Manual de “Políticas y Normas de Seguridad de la Información” del Instituto Nacional de Vías INVIAS, para plantear su actualización de acuerdo con el modelo MSPI y reglamentado por el “Modelo de Seguridad y Privacidad” de Gobierno en Línea (GEL) y de los estándares actuales.

OBJETIVOS ESPECÍFICOS.

- Identificar el activo informático que se va a proteger bajo el esquema normativo de seguridad GEL/ISO 27001:2013 y las áreas susceptibles de ataques o con problemas de seguridad dentro del INVIAS.
- Identificar las amenazas y debilidades del actual sistema de manejo y protección de la información. Metodología Magerit, actualizada en versión 3. Anexo Final.
- Diagnosticar las "Políticas de Seguridad", privacidad y manejo de la información, existentes con las ajustadas a los estándares internacionales actuales.
- Elaborar Un documento final que incluya las actualizaciones, recomendaciones y formulaciones sobre "Políticas de Seguridad de la Información", de tal manera que puedan ser aprobada y adaptadas por el Instituto Nacional de Vías, INVIAS. Anexo Final.

RESUMEN DE LO DESARROLLADO EN EL PROYECTO.

- **Identificación de Activos del Instituto Nacional de Vías. INVIAS, planta central**

Con la autorización y aval del Instituto Nacional de Vías. INVIAS, planta central, se procedió a elaborar un diagnóstico inicial de las Políticas de la Información de la entidad y así identificar el tipo de amenazas, riesgos y responsabilidades a la que se ve expuesta el activo informático de la entidad como lo es la Información.

Al tener siempre presente el concepto de seguridad, implementando la actualización de las políticas existentes y abordando en nuevas, para que con el debido tratamiento de la información los activos informáticos no sean frágiles y estén prestos a un sistema de gestión de la Seguridad de la Información, con calidad, eficacia y eficiencia.

- **Vulnerabilidades y amenazas.**

- Una vez aborda la normatividad vigente para el estudio y el referente histórico de los efectos administrativos y económicos, se da conocer la importancia de las normas en la búsqueda de medidas a los efectos de la dinámica de trabajo que realiza las Políticas de Seguridad de la Información al interior del Institutito Nacional de Vías. INVIAS, planta central. Como se expone con la utilización de la metodología Magerit.

- **Recopilar información de las metodologías de Ingeniería Social**

Para aplicar el análisis general a la documentación, exponer las entrevistas y formatos existentes, se revisan dentro del contexto estratégico organizacional, mejoras en la Caracterización de proceso y demás documentos relacionados con la Gestión de Tecnologías de Información y de Comunicación; Alineación GEL , Seguridad de la Información en el Instituto Nacional de Vías-INVIAS-Planta Central, así como también las estrategias y el cómo aplicarlas en el proyecto para lograr identificar hasta donde es vulnerable la entidad, sin una actualización de las Políticas de Seguridad de la Información.

- **Determinar metodologías de Ingeniería social**

Se procede a realizar las respectivas fases del proyecto, pruebas de Ingeniería social, para el logro de los objetivos propuestos, en razón al proceder a realizar las respectivas fases del proyecto, pruebas de Ingeniería Social para el logro de los objetivos propuestos, en razón Estudio y Diagnostico de Políticas de Seguridad de la Información, para el Instituto Nacional de Vias. INVIAS, nivel central.

1. La primera fase analiza la documentación, identifica los activos informáticos de la entidad, INVIAS, la documentación con la información que se relaciona con la temática propuesta de investigación del tema, como todos aquellos procedimientos, normas, leyes, resoluciones, políticas implementadas que rigen para la entidad.

   El análisis anterior contempló datos como: número de usuarios, servidores, terminales de trabajo, software, licencias etc. Soporte de la información mediante entrevista al ingeniero de soporte tecnológico, sobre virtudes y falencias del sistema, la estructura e infraestructura tecnológica, los riesgos sobre seguridad física y del entorno de la seguridad informática, el crecimiento de la infraestructura de la entidad, Instituto Nacional de Vías, INVIAS. Todo esto como base para la generación de las nuevas Políticas de Seguridad de la Información, aprobadas por la alta dirección de la entidad.

2. La segunda Fase: Se Generó, Organizo y tabulo, lo referente a la información recolectada sobre la infraestructura informática y la información, para el diagnóstico inicial. Igualmente los factores de amenazas y protecciones utilizadas, el mapa de procesos de la Entidad Instituto Nacional de Vias-INVIAS y la documentación jurídica, como también lo existente frente a la norma NTC 27000 y la estrategia GEL.

3. La tercera Fase: Se elabora un diagnóstico de las “Políticas”, identificando la existente, el manejo de la misma y la seguridad de la información, asumiendo tareas de identificación y clasificación de las mismas.

4. La Cuarta Fase: Se relaciona las tecnologías, estándares y elaboración del documento final, en el que se toman en cuenta los diferentes grupos de la oficina de sistemas del INVIAS, tales como, Plataforma Tecnológica, Soporte y Control y Sistemas de Información, y según su organización.

- **Generar el estudio y Diagnostico de las Políticas de Seguridad de la Información existentes, para el Instituto Nacional de Vías. INVIAS, Planta central.**

Se diseña con el fin de elaborar las recomendaciones e implementar las nuevas estrategias en relación a la prevención de delitos informáticos, perdida de información y así fomentar cultura social y educativa, a los empleados contratistas y usuarios externos del Institutito Nacional de Vías-INVIAS. este manual se entregó impreso en la Institución, al igual quedo plasmado en la página web institucional

- **Capacitaciones al personal**

La entidad se compromete a la difusión e implementación del estudio y diagnóstico de las políticas de seguridad una vez revisadas, para su socialización a los Funcionarios, Contratistas y Personal externo de la entidad. Como también estrategia de apoyo en las capacitaciones que se elaboran,

al interior de la entidad y para que el funcionario en general, sea consiente de cómo debe actuar ante las diversas estrategias Políticas de Seguridad de la Información y los elementos que pueden poner en riesgo la confiabilidad de la información y así lograr prevenir que cualquiera al interior de la entidad, sea víctima de la de virus o ataques informáticos en general.

METODOLOGÍA DE DESARROLLO

En cuanto al objetivo general del proyecto, un Análisis de resultados facilita la actualización y mejora al documento Manual de Políticas y Normas de Seguridad de la Información en el Invias, una versión actualizada de los riesgos, amenazas y peligros a que se puede ver expuesta la información y los activos informáticos del Instituto Nacional Vías Invias. Y de acuerdo con el modelo MSPI y reglamentado por el Modelo de Seguridad y Privacidad de Gobierno en Línea (GEL) y de los estándares actuales.

- Para el segundo objetivo y una vez logrado el objetivo general del proyecto se trabajan los planteamientos sobre el Análisis del documento Manual de Políticas y Normas de Seguridad de las información en el Invias, se identificaron los activos informáticos que se van a proteger bajo el esquema normativo de seguridad GEL/ISO 27001:2013 y las áreas susceptibles de ataques o con problemas de seguridad dentro del INVIAS.

- Al tener conocimiento del activo informático que se va a proteger bajo el esquema normativo de seguridad GEL/ISO 27001:2013, unas políticas actualizadas identifican las amenazas y debilidades del actual sistema de manejo y protección de la información, del Instituto Nacional De Vías. Por lo que al diagnosticar las Políticas de Seguridad, Privacidad y Manejo de la Información existentes con las ajustadas a estándares internacionales actuales, dará una mejor oportunidad de eficiencia y eficacia a la entidad, solucionando en buena parte los problemas de seguridad dentro del INVIAS.

- Con el último objetivo e identificas las amenazas y debilidades del actual sistema de manejo y protección de la información, en el Invias se logra diagnosticar los problemas que surgen en cuanto a la protección de la información y los activos informáticos. Por los que las Políticas de Seguridad, Privacidad y Manejo de la Información existentes con las ajustadas a estándares internacionales actuales,

Este objetivo se entregara impreso al Instituto Nacional de Vías Invias, la elaboración del documento final que incluye las recomendaciones y formulaciones sobre Políticas de Seguridad de la Información de tal manera que puedan ser aprobadas y adaptadas por el Instituto Nacional de Vías, INVIAS, planta central.

Conclusiones

1. ajustar de manera inmediata el actual Manual de Políticas de Seguridad, Privacidad y Manejo de la Información existentes con las ajustadas a estándares internacionales actuales. Trabajar en pro de la nueva actualización del Manual de Políticas de Seguridad de la Información, con la Dirección y la Oficina de Planeación Institucional, para así, hacer partícipe a los líderes de procesos/subprocesos en el ajuste e implementación de estas políticas, al 2018.

2. Se debe Instruir de manera adecuada sobre la nueva metodología Estrategias para la socialización de las Políticas de Seguridad de la Información, del Instituto Nacional de Vías. INVIAS, planta central.

3. El Modelo de Seguridad y Privacidad de GEL y la madurez del modelo en el INVIAS, recomienda que se debe implementar de inmediato a todos los indicadores generados en este proyecto, con el fin de generar registros en cada uno de ellos.

4. Aplicando la revisión, estudio y diagnóstico de la información sobre estrategias de ingeniería social se logró identificar el nivel de riesgo y vulnerabilidad en la que se encuentra la información como activo informático de la entidad, en donde se concluye que cualquier puede capturar la información bajo un rol indebido.

5. Que todavía se encuentran personas en la entidad con escasos conocimientos en el manejo del ámbito informático, que se observa, con el desarrollo de la encuesta y la práctica que se llevó a cabo.

6. El compromiso mayor de las directivas de la entidad en establecer e identificar los problemas y así establecer la vía para la difusión e implementación del estudio y diagnóstico de las políticas de seguridad una vez revisadas, para su socialización a los funcionarios, Contratistas y Personas externas de la entidad, Instituto Nacional de Vías. INVIAS, planta central.

Recomendaciones.

- ✓ Las principales recomendaciones realizadas son:
- ✓ Observar y monitorear los indicadores creados de acuerdo con los registros generados, con el fin de verificar si el objetivo del indicador se cumple o si el mismo requiere un ajuste de acuerdo a su comportamiento.
- ✓ Controlar el Tiempo que lleva la implementación del proyecto.
- ✓ El Dominio de la Norma ISO/IEC 27001:2013.
- ✓ Vigilar roles para llevar a cabo la implementación y/o monitoreo del presente proyecto.
- ✓ Incorporar con prontitud el proceso de inducción a los funcionarios en la divulgación de las funciones y responsabilidades frente a la seguridad de la información desde su vinculación, hasta su desvinculación.
- ✓ Incorporar con prontitud el proceso de inducción a los funcionarios en la divulgación de las funciones y responsabilidades frente a la Seguridad de la Información seguridad de la información desde su vinculación, hasta su desvinculación.
- ✓ Revisar periódicamente el nivel de apropiación de la actualización del manual Modelo de Seguridad y Privacidad de la Información a funcionarios, contratistas y terceros, a través de métricas, con el fin de identificar la necesidad de reforzar las charlas, sesiones de trabajo, talleres y herramientas utilizadas.
- ✓ Identificar temas de interés afines con la Seguridad de la Información, que ayuden de primera mano a reconocer los estándares internacionales y buenas prácticas aplicables al instituto, en lo que refiere al nuevo y actualizado Manual de Políticas de Seguridad de la Información.
- ✓ En cuanto a los puntos de red del cableado estructurado con que cuenta el Instituto Nacional de vías-INVIAS, que se encuentran al alcance de cualquier persona se aconseja mantener esta infraestructura protegida y segura.