PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Elaborado por: Ing. JUAN CARLOS PUENTES G

Profesional Especializado-Sistemas

Tunja, 28 de enero de 2.019

TABLA DE CONTENIDO

CONTENIDO

1. TABLA ILUSTRACIONES

2. TABLA DE TABLAS

3. TABLA DE ANEXOS

Anexo A MN-GET-0-01 Política General Seguridad de la Información

Anexo B MN-GET-0-02 Política Particular Publicación Sitios Web

Anexo C MN-GET-0-03 Política Particular Información Contenida en los Computadores

Anexo D MN-GET-0-04 Política Particular Uso de Cuentas De Usuario

Anexo E Resumen-Indicadores

Anexo F Cuadro-Indicadores

Anexo G Análisis-Costos-Incidentes

Anexo H Matriz Análisis-De Riesgo

4. RESUMEN

Parte fundamental de un sistema de Gestión de Seguridad de la información, es la elaboración de una adecuada gestión de riesgos, que le permita a la organización identificar de manera plena las vulnerabilidades de sus activos de información y las amenazas que pudieran generarse por las debilidades en el sistema, de tal manera que se puedan crear medidas preventivas y correctivas que garanticen la seguridad de la información. Un factor común de todas las metodologías para la gestión del riesgo es la identificación de los activos de información que no son otros diferentes a las herramientas utilizadas para la gestión de la información, por tanto hacen parte de estas, los datos, hardware, recurso humano e información escrita; partiendo de este concepto puede entonces definirse como amenaza según (Luján) "a todo elemento o acción capaz de atentar contra la seguridad de la información. Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.

Diversas situaciones, tales como el incremento y el perfeccionamiento de las técnicas de ingeniería social, la falta de capacitación y concientización a los usuarios en el uso de la tecnología, y sobre todo la creciente rentabilidad de los ataques, han provocado en los últimos años el aumento de amenazas intencionales".

Ahora bien, no pueden dejar de tenerse en cuenta otros conceptos igualmente importantes como son la definición de vulnerabilidad la cual según (seguridad, s.f.) Es "una vulnerabilidad informática es un elemento de un sistema informático que puede ser aprovechado por un atacante para violar la seguridad, así mismo pueden causar daños por sí mismos sin tratarse de un ataque intencionado.

A las vulnerabilidades se les consideran un elemento interno del sistema, por lo que es tarea de los administradores y usuarios de la organización el detectarlos, valorarlos y reducirlos.

Parte fundamental de un sistema de Gestión de Seguridad de la información, es la elaboración de una adecuada gestión de riesgos, que le permita a la organización identificar de manera plena las vulnerabilidades de sus activos de información y las amenazas que pudieran generarse por las debilidades en el sistema, de tal manera que

se puedan crear medidas preventivas y correctivas que garanticen la seguridad de la información. Un factor común de todas las metodologías para la gestión del riesgo es la identificación de los activos de información que no son otros diferentes a las herramientas utilizadas para la gestión de la información, por tanto hacen parte de estas, los datos, hardware, recurso humano e información escrita; partiendo de este concepto puede entonces definirse como amenaza según (Luján) "a todo elemento o acción capaz de atentar contra la seguridad de la información. Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.

Diversas situaciones, tales como el incremento y el perfeccionamiento de las técnicas de ingeniería social, la falta de capacitación y concientización a los usuarios en el uso de la tecnología, y sobre todo la creciente rentabilidad de los ataques, han provocado en los últimos años el aumento de amenazas intencionales"

Ahora bien, no pueden dejar de tenerse en cuenta otros conceptos igualmente importantes como son la definición de vulnerabilidad la cual según (seguridad, s.f.) Es "Una vulnerabilidad informática es un elemento de un sistema informático que puede ser aprovechado por un atacante para violar la seguridad, así mismo pueden causar daños por sí mismos sin tratarse de un ataque intencionado.

A las vulnerabilidades se les consideran un elemento interno del sistema, por lo que es tarea de los administradores y usuarios de la organización el detectarlos, valorarlos y reducirlos.

Palabras clave

Riesgos, amenazas, indicadores, vulnerabilidades, activos de información, debilidades, ataques, valoración, controles, métricas, incidentes, gestión.

3. ALCANCE

A través de este documento se pretende analizar los riesgos y amenazas del proceso estratégico de Comunicación, que contempla los lineamientos establecidos para regular las comunicaciones tanto internas (cliente interno, es decir, al trabajador y tiene como fundamento fortalecer las habilidades comunicativas), como externas (dirigida a los usuarios de los servicios de Registro de tránsito y de las vías de jurisdicción del ITBOY (conductores, pasajeros, y peatones); que apoyan la misión institucional frente al tema de seguridad vial de influencia del ITBOY).

De igual manera las siguientes actividades que se pretenden desarrollan en este son:

- Identificación y análisis de los activos de información que se encuentran contemplados en el proceso estratégico de comunicación del ITBOY, utilizando la metodología de análisis y Gestión de Riesgos de los sistemas de información de Magerit V.3.
- Identificación, valoración y evaluación de los riesgos a lo que se exponen los activos de información del ITBOY.
- Establecer y priorizar las amenazas y riesgos de seguridad dela información para diagnosticar, evaluar y comunicar el nivel de exposición del ITBOY, a través de la metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de Magerit v.3.
- Informe de análisis de riesgos realizado.
- Matriz de controles aplicados al proceso de negocio Comunicaciones.
- Identificación y clasificación de métricas e indicadores para el sistema de gestión de seguridad de la información del proceso estratégico de Comunicaciones del ITBOY.
- Valoración cualitativa y cuantitativa de los incidentes de seguridad de la información.
- Análisis de costos de los incidentes de seguridad más frecuentes según Kaspersky, utilizando el modelo Ponemon.
    - Análisis de los riesgos emergentes utilizando la herramienta Ventana de AREM, que permita al IDS, tomar decisiones frente a las situaciones inesperadas y desconocidas que se pueda enfrentar.

5. INTRODUCCIÓN

El tema objeto de esta documento está orientado a la evaluación del sistema de Gestión de seguridad de la información del Instituto de Tránsito de Boyacá - ITBOY, a efectos de generar una propuesta estratégica y táctica al nivel directivo facilitando de esta manera la toma de decisiones, la cual permitirá la mejora continua en el cambio de panorama de los riesgos de TI., fortaleciendo el proceso de comunicación que hace parte del sistema de Gestión.

Se plantearan elementos propios del direccionamiento estratégico de la seguridad de la información apoyado en políticas, estándares procedimientos para la protección de la información.

Por otra parte, al diagnosticar, evaluar y comunicar el nivel de exposición a los riesgos y amenazas de la información en el ITBOY, motivará a la alta gerencia así como a los empleados a proteger la información.

Analizaremos los riesgos emergentes con la ventana de Harem, como una herramienta estratégica y táctica para visualizar la incertidumbre abarcando las áreas de: libre, oculta, ciega y desconocida.

Este ejercicio académico nos permitirá comprender el valor estratégico de la información, los posibles riesgos y amenazas, diseñar políticas específicas y generales acordes a los objetivos institucionales, planes de tratamiento de riesgos, aspectos claves para medir, acciones y análisis de riesgos emergentes, cuantificación y valoración de incidentes de seguridad, indicadores, métricas, controles para mantener la seguridad de la información y análisis de riesgos emergentes.

Como marco de referencia nos apoyamos en los diferentes estándares actualmente reconocidos como son ISO 27001:2013, 27002:2005, 27032:2012, 38500:2008, ITIL, ISM3, para abordar la necesidad de implementar un sistema de gestión de seguridad de la información (SGSI) en las organizaciones, en nuestro caso de estudio es el ITBOY lo utilice al evaluar, dirigir y monitorear el uso de las tecnologías de la información (TI's).

También se afianzarán los conceptos que ayudarán al análisis estratégico y crítico para orientar a los directivos del ITBOY, en la toma de decisiones de una manera alineada a los objetivos institucionales, generando valor agregado referenciador.

6. DESCRIPCIÓN DE LA EMPRESA

INSTITUTO DE TRÁNSITO DE BOYACÁ - IT BOY.

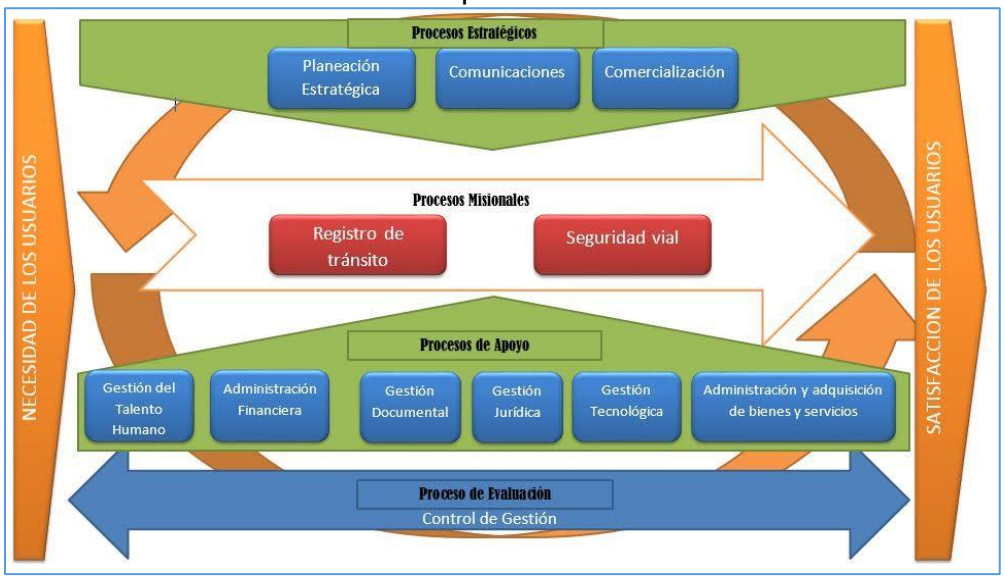
Tabla 1. Generalidades de la Entidad.

Entidad seleccionada	**IT BOY – INSTITUO DE TRÁNSITO DE BOYACÁ**
Tipo de Organización	PÚBLICA DEL ORDEN DEPARTAMENTAL
Ubicación	Calle 2 #72-43, Tunja, Boyacá
Sector:	Transporte
Creada:	En 1975, con la ordenanza 044 del 28 Noviembre

Fuente. Elaboración propia.

6.1.1 Descripción: El Instituto de Tránsito de Boyacá (ITBOY), es un establecimiento público departamental, de carácter técnico encargado de gestionar el manejo y administración del registro de tránsito y la seguridad vial. Lo anterior de acuerdo a los Decretos 01517 y 1686 de 1995 y 2001 respectivamente.

Ilustración 1. Mapa de Procesos ITBOY



Fuente. http://www.itboy.gov.co

6.1.2 Objetivos estratégicos.

- Poner en marcha las líneas estrategias que consagra el Plan Departamental de Seguridad Vial contenidas en la Ordenanza 025 de 2010 y Resolución 086 de 2011 del ITBOY.
- Adelantar convenios o alianzas estratégicas, con entidades del orden Municipal, Departamental y/o Nacional, con el fin de desarrollar los proyectos del Plan Departamental de Seguridad Vial.
- Velar por la seguridad vial de las personas y objetos en la jurisdicción del ITBOY mejorando la movilidad en las vías.
- Prestar asistencia técnica y humana a los usuarios de las vías.
- Satisfacer las necesidades y expectativas de los usuarios y demás partes interesadas.

6.1.3 Planeación estratégica

6.1.3.1 Política de Calidad

El Instituto de Tránsito de Boyacá - ITBOY, se compromete a generar condiciones para mejorar la Seguridad Vial y administrar el registro de tránsito, con tecnología avanzada, con personal calificado, orientado hacia la satisfacción de las necesidades y expectativas de sus usuarios y demás partes interesadas, con un Sistema de Gestión de Calidad que garantice la mejora continua de sus procesos con eficacia, eficiencia y efectividad, para contribuir con el logro de los fines del estado".

6.1.3.2 Principios

La información que procesa y produce el Instituto de Tránsito de Boyacá es un bien público.

- En el Instituto de Tránsito de Boyacá los bienes públicos son sagrados.
- La razón de ser del funcionario público es servir a la ciudadanía.
- El Instituto de Tránsito de Boyacá promueve el desarrollo integral de su talento humano para fortalecer el sentido de pertenencia y el mejoramiento continuo en la atención a sus usuarios.

- En el Instituto de Tránsito de Boyacá se promueve la transparencia en la gestión pública, fortaleciendo el control social, mediante la difusión de la información pertinente.
- En el Instituto de Tránsito de Boyacá el interés general prima sobre el interés particular.
  - **Valores :**Los valores institucionales que inspiran y soportan la gestión del Instituto de Tránsito de Boyacá son:
  - **Eficiencia:** El Instituto de Tránsito de Boyacá es una entidad eficiente, que tiene la capacidad de cumplir su misión institucional con el mejor uso de los recursos.
  - **Compromiso:** El compromiso del Instituto de Tránsito de Boyacá con su misión y con la comunidad se evidencia en la voluntad de sus servidores públicos por alcanzar con niveles de excelencia, el logro de los objetivos del estado.
  - **Respeto**: El Instituto de Tránsito de Boyacá reconoce los derechos de los clientes internos y externos y trabaja para lograr el fortalecimiento y mejoramiento de sus obligaciones y comportamientos. Los servidores públicos aceptan las sugerencias de sus compañeros y de las entidades del ámbito de aplicación, que les permite interactuar en forma eficiente con la prestación de los servicios.
  - **Honestidad:** En el Instituto de Tránsito de Boyacá obramos de acuerdo con los principios fundamentales que rigen el respeto por el ser humano y los ciudadanos, en particular, actuando de manera transparente en la utilización de los bienes del estado, y en el cumplimiento de nuestras obligaciones, lo que nos permite el desarrollo institucional y la convivencia ciudadana.
  - **Transparencia:** El Instituto de Tránsito de Boyacá es una entidad transparente, dispuesta a ser observada por las demás instituciones públicas, por la comunidad y la ciudadanía en particular, en el cumplimiento de sus funciones, las cuales se fundamentan en los conceptos de oportunidad y veracidad.

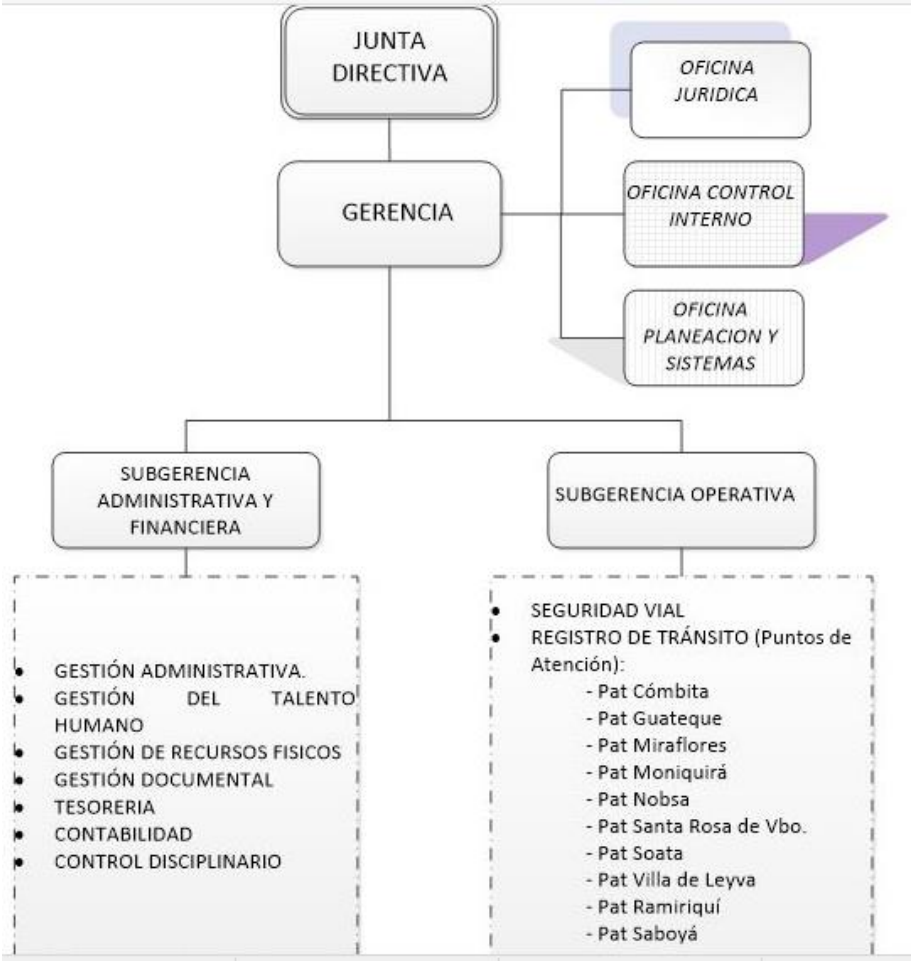
- **Servicio:** El Instituto de Tránsito de Boyacá se caracteriza por la satisfacción a los usuarios internos y externos, de sus necesidades a nivel social, técnico, financiero y de calidad en la información.

6.1.3.3 Misión: El Instituto de Tránsito de Boyacá (ITBOY) coordina la seguridad y movilidad vial en el área de influencia del Instituto en el departamento de Boyacá y administra el registro de tránsito, con personal calificado y comprometido con la institución y puntos de atención autorizados por el Ministerio de Transporte, para contribuir con el incremento de la calidad de vida de los actores viales e intereses de los usuarios.

6.1.3.4 Visión: El Instituto de Tránsito de Boyacá (ITBOY), se proyecta para hacer de Boyacá en el 2025, el departamento con las vías más seguras del país y con el mejor portafolio de servicios de Tránsito, soportado en su recurso humano y tecnológico, capaz de materializar su misión Institucional.

6.1.3.5 Quiénes Somos: El Instituto de Tránsito de Boyacá (ITBOY), es un establecimiento público del departamento, de carácter técnico encargado de gestionar el manejo y administración del registro automotor y la seguridad vial a nivel departamental, de conformidad con lo previsto en el Decreto 01517 de 1995 y en los términos y condiciones previstos en el Decreto 1686 del 30 de noviembre de 2001.

Ilustración 2. Organigrama del ITBOY



Fuente. Sistema de Gestión de calidad del ITBOY

6.1.4 Plan integral de desarrollo

ITBOY, tiene como uno de sus ejes misionales dentro del plan de desarrollo (2016-2019) asegurar todos los registros de tránsito del área de su influencia. Sin embargo, en este se identificó que uno de los principales problemas referentes a la gestión de información de tránsito se encuentra en la diversidad de documentos en físico en donde se hace constancia de múltiples trámites que se realizan día a día por usuarios y la entidad; es entonces, deber del ITBOY, asegurar la adecuada custodia y registro de toda la documentación recibida.

De igual forma, en el documento oficial del Plan de desarrollo ITBOY se describen algunos subprogramas que van de la mano con el lineamiento estratégico general del departamento de Boyacá entre ellos:

- **Programa Modernización institucional:** Fortalecer el Sistema de Gestión Documental, sistematizar y modernizar los procesos documentales de la entidad, mediante la implementación de nuevas tecnologías para un manejo seguro y transparente de la información.
- **Programa de Vigilancia y Control:** el cual tiene como objetivo prevenir la accidentalidad y promover el respeto por las normas de tránsito.
- **Programa de Articulación interinstitucional:** Que tiene como objetivo Vincular entidades públicas y/o privadas al Plan Departamental de Seguridad Vial (PDSV). Generando responsabilidad social planificando mecanismos, estrategias y medidas que originen conciencia frente a la prevención de accidentes de tránsito, por medio de sensibilización y capacitación.
- **Programa de Señalización vial:** Señalizar las vías del departamento ITBOY, Teniendo en cuenta los factores básicos de tránsito, establecidos en el Plan Nacional de Seguridad Vial: ser humano, vehículo y entorno.
- **Sensibilización en cultura vial:** Sensibilizar a la población del departamento en cultura y convivencia vial.
- **Sensibilización a motociclistas:** Concientizar a los motociclistas entorno al cumplimiento de las normas de tránsito.

6.1.5 Estado de SGSI

Actualmente el ITBOY, cuenta con una política de gestión de seguridad de la información SGSI en donde se definen de forma global algunas normas, parámetros, responsabilidades y directrices.

Se tienen documentos en donde se plasman las políticas de administración de usuarios y servicios de red, planillas para asignación y direccionamiento de IP; no se encuentran bajo la Norma ISO 27001 de 2013 y del Modelo de Seguridad y Privacidad de la Información (MSPI).

Basado en el análisis realizado a la política existente en ITBOY, podemos definir que el documento vigente está enfocado a temas netamente técnicos (router para bloquear posibles intento de penetración en la red, módulos de IPS y IDS, sistemas de información, desarrollos open source, creación de usuarios); siguiendo los lineamientos y estándares vigentes dentro de esta política general deberíamos encontrar y definir puntos estratégicos que apalanquen los objetivos estratégicos de ITBOY de una forma segura y estándar. Por lo cual se propone en este ejercicio educativo, redefinir la política general de ITBOY para que esta sea validada por la alta gerencia para el cumplimento de los lineamientos basados en los estándares de seguridad de la información.

6.1.6 Análisis de la Empresa

El Ministerio de Transporte, como lo establece el Decreto 087 de 2011, es el organismo del Gobierno Nacional encargado de formular y adoptar las políticas, planes, programas, proyectos y regulación económica del transporte, el tránsito y la infraestructura, en los modos carretero, marítimo, fluvial, férreo y aéreo del país.

Por lo anterior, el Ministerio delega en los organismos de tránsito y transporte, a nivel nacional, las funciones de controlar todo lo relacionado con el registro de tránsito y transporte y en el caso del Instituto de tránsito de Boyacá “ITBOY”, lo referente a tránsito y seguridad vial que es el deber ser y por ende sus procesos misionales, como se describe en el sistema de gestión de calidad "coordinar la seguridad y movilidad vial en el área de influencia del Instituto en el departamento de Boyacá y administrar el registro de tránsito, a través de los puntos de atención autorizados por el Ministerio de Transporte, para contribuir con el incremento de la calidad de vida de los actores viales e intereses de los usuarios" .

Ahora bien, en el año 2009 por disposición del ministerio del transporte todos los organismos de tránsito del país deberían migrar todos los registros producto de la captura de los historiales de vehículos a las nuevas bases de datos del naciente Registro Único Nacional de Tránsito "RUNT", este proceso para el ITBOY fue traumático por la presión ejercida por los entes de control y la posible sanción, ya que los tiempos establecidos para alcanzar esta meta fueron insuficientes, lo que conllevo a una nada confiable captura de los registros.

Esta situación conlleva a procesos engorrosos, demorados y nada confiables cuando se requiere realizar un trámite de tránsito especialmente, para el caso de los traspasos, ya que se requiere de una verificación en físico del historial, consulta esta que implica la exposición de la carpeta (en algunas ocasiones sin gestión documental) corriendo el riesgo de adulteración de los documentos o pérdida de los mismos.

Las instituciones de carácter gubernamental (públicas) como lo es el ITBOY, tienen la obligación de hacer públicos sus actos y de garantizar la exposición de los documentos también considerados como públicos, como lo contempla la ley de transparencia (Congreso de la República, 2014) en los artículos 1 y 2 así:

Artículo 1°. Objeto. El objeto de la presente ley es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.

Artículo 2°. Principio de máxima publicidad para titular universal. Toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal, de conformidad con la presente ley".

Cero Papel: De acuerdo con (Archivo General de la Nación, 2012), la circular 005 del archivo general de la nación ilustra el siguiente concepto:"La *"Iniciativa Cero Papel"* es una directriz del Gobierno Nacional enmarcada dentro del Plan Vive Digital y en cuyo desarrollo participan además del Programa Gobierno en Línea del Ministerio de Tecnologías de la Información y las Comunicaciones, el Archivo General de la Nación, la Alta Consejería para el Buen Gobierno y el Departamento Administrativo de la Función Pública.

En este contexto, la Presidencia de la República expidió la Directiva Presidencial 04 de 2012, mediante la cual se solicita a las entidades públicas la reducción del papel como medio de registro de documentos y actuaciones de la administración pública, adoptando diferentes prácticas así como la utilización de medios electrónicos en la gestión documental del Estado. De igual forma, en el marco del Decreto - Ley 019 de 2012 (Congreso de la República, 2012) *"Ley Antitrámites",* la iniciativa se debe entender

como un apoyo para racionalizar y simplificar trámites, procesos, procedimientos y servicios internos, con el propósito de eliminar funciones y barreras que impidan la oportuna, eficiente y eficaz gestión de las entidades."

Por lo expuesto anteriormente, en el Instituto se evidencia una debilidad que puede catalogarse como crítica y un riesgo latente por el incumplimiento de las normas establecidas por el gobierno nacional mediante los leyes citadas anteriormente, frente a la oportunidad, confiabilidad, transparencia y políticas de cero papel, e incluso en temas penales que pueden se motivados por falta de mecanismos de seguridad que protejan la información contenida en los históricos de los vehículos.

Sin embargo en el plan de desarrollo la entidad intenta subsanar esta falencia mediante la formulación de proyectos cuyo objeto es la digitalización para propiciar el archivo electrónico y la consulta en línea.

4.1.6.1 Relación entre el sistema de gestión de seguridad de la información y planeación estratégica.

Si bien es cierto, el Instituto cuenta con documentos como el identificado “MN-GET-01 POLÍTICAS SEGURIDAD INFORMÁTICA", donde se contemplan lineamientos propios de la institución tendiente a plasmar las directrices encaminadas a asegurar los sistemas de información, no se observa una relación con el proceso de gestión documental.

En el cuerpo de este documento se plantea una mejora en temas de seguridad informática que buscan subsanar las falencias encontradas en el diagnóstico de la entidad, y una correlación entre este y la información estratégica organizacional.

7. ANÁLISIS POLÍTICAS DE SEGURIDAD.

Luego de realizar investigación y análisis de las políticas de seguridad a nivel general para las compañías INVIMA (Colombia), INTECO (España), Presidencia de la Republica (Colombia), se validaron diversos factores y la relevancia que tienen estos sobre la protección de la información misional de las compañías para las cuales fueron desarrollados, pues permite salvaguardar de cualquier modo los intereses de las empresas y de esta forma garantizar la integridad, confidencialidad y disponibilidad de la misma. En la actualidad ITBOY cuenta con documentación

técnica que permite conocer internamente algunos procesos, sin embargo no cuenta con la implementación y desarrollo de políticas que salvaguarden el core de su negocio y que garanticen la segura ejecución del mismo, motivo por el cual se realizó un análisis grupal de la situación y se determinó proponer a la dirección de la entidad dar inicio a la implementación del sistema de gestión seguridad de la información y elaborar las políticas que lo componen garantizando el cubrimiento de los procesos que ejecuta la entidad y con la aprobación de la entidad comenzar a trabajar internamente en la concienciación acerca de la importancia de su ejecución.

7.1.1 Proceso Estratégico Comunicaciones

Plantear el proceso de comunicaciones como parte fundamental en los procesos del Instituto, parte del principio de que como seres sociales, necesitamos estar comunicándonos, es entender que la comunicación es clave en la construcción de las organizaciones.

El proceso de comunicaciones, es fundamental para regular, planear y desarrollar políticas, que permitan el control total de los medios, a fin de fortalecer la interrelación en los temas de interés público y la generación de confianza entre los actores.

El plan estratégico de comunicaciones es un proceso integral que recoge políticas, recursos, procedimientos y acciones a desarrollar a fin de involucrar todos los demás procesos del ITBOY.

Dada la importancia de este proceso, se pretende fortalecer la política de comunicaciones en procura de la mejora continua que debe ser estandarte de las entidades del estado para garantizar la transparencia y las buenas gestiones.

Objetivo: Establecer los canales y usos informativos institucionales más apropiados para la divulgación de la información del Instituto, bien sea desde el escenario de la comunicación interna o externa, y de éste modo mantener informado y actualizado frente a los temas de interés al público.

Alcance: Inicia con la identificación de la información a comunicar, y termina con la publicación y/o entrega de la misma al interesado. Aplica para los proceso del Instituto y demás partes interesadas.

El proceso contempla los lineamientos establecidos para regular las comunicaciones tanto internas (dirigida al cliente interno, es decir, al trabajador, y tiene como fundamento fortalecer las habilidades comunicativas a nivel interno, para evitar la incomunicación y promover un buen ambiente corporativo) como las comunicaciones externas (dirigida a los usuarios de los servicios de Registro de tránsito y de las vías de jurisdicción del ITBOY (conductores, pasajeros, y peatones) y tiene como fundamento apoyar la misión institucional frente al tema de seguridad vial en las vía de influencia del ITBOY). El proceso involucra un manual de comunicaciones MN-COM-01, ficha de caracterización (indicadores, FR-CDG-13 MAPA DE RIESGOS), 6 formatos (FR-COM-01 CONTROL DE PUBLICACIÓN PAGINA WEB,FR-COM-02 SOLICITUD DE AUTORIZACIÓN PARA LA ENTREGA MASIVA DE MATERIAL FÍSICO O DIGITAL SIN RADICADO,FR-COM-03 SOLICITUD PUBLICACIÓN EN CARTELERAS FÍSICAS Y O DIGITALES,FR-COM-04 SOLICITUD EMISIÓN DE MENSAJES INSTITUCIONALES EN MEDIOS DE COMUNICACIÓN MASIVOS,FR-COM-05 SOLICITUD PARTICIPACIÓN DE FUNCIONARIOS EN MEDIOS MASIVOS O ALTERNATIVOS DE COMUNICACIÓN,FR-COM-06 VERIFICACIÓN DE PARTICIPACIÓN EN MEDIOS DE COMUNICACIÓN),OD-COM-01 MATRIZ INFORMATIVA ITBOY y un procedimiento:PD-COM-01 - PROCEDIMIENTO DE COMUNICACIONES INTERNAS Y EXTERNAS

7.1.2 Generación Política General SGSI

Basados en la información y documentos recolectados por el grupo de trabajo en ITBOY, se define hacer una propuesta para redefinir la política actual del SGSI, esta se fundamenta en el hecho de que actualmente no se encuentra alineada con los objetivos estratégicos de ITBOY. Para esta labor nos basamos en la triada GRC (Gobierno, Riesgos y Cumplimiento) con la cual se llevara a cabo la identificación de la ruta a seguir de acuerdo a los objetivos estratégicos de la entidad.

Ilustración 3. Triada GRC para el ITBOY

Fuente. Elaboración Propia.

Por lo anterior, se procederá a redefinir la política de SGSI de forma que esté alineada con el objetivo estratégico de **comunicaciones** encargado de satisfacer las necesidades y expectativas de las partes interesadas, referente a la divulgación de la información institucional a través de los canales de comunicación como son: Redes Sociales, Sitio Web, Portafolio de Servicios, Carteleras Informativas, Prensa y Emisoras Radiales.

Desde la Dirección de ITBOY se plantea:

- Redefinir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en directrices claras establecidas con la misión, visión, principios, valores, funciones, servicios y objetivos estratégicos de la Institución.
- Definir un grupo conformado estratégicamente que permita además de planear, ejecutar y hacer seguimiento de las acciones definidas con anterioridad basado en un cronograma de actividades.
- La alta dirección de ITBOY al igual que los coordinadores y jefes de área se encuentran comprometidos en la divulgación y cumplimiento tanto de la política general de SGSI como de las políticas generales a saber:

Política General de la Seguridad de la información

La dirección del Instituto de Tránsito de Boyacá **(ITBOY)**, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad estableciendo los lineamientos y controles de seguridad de la información necesarios para proteger la confidencialidad, integridad y disponibilidad de la información propiedad de **ITBOY** y de sus clientes apoyados en estándares y buenas prácticas de seguridad de la información.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI.

Generación Políticas Particulares

- **Política Uso Cuentas de Usuario:** Aplica para todos los funcionarios Y contratistas, cuyas actividades de administración del sistema, de gestión o cualquier otro acceso que esté permitido para las contraseñas de sistema de los recursos del ITBOY, como: servicios Web, cuentas de correo electrónico, protectores de pantalla, en los recursos de los usuarios, administración de dispositivos remotos.
- **Política Manejo de Información contenida en los Computadores:** Esta política particular determinar el uso de la información contenida en los computadores, por los usuarios de la red del ITBOY.

- **Política Publicación Sitios Web:** Aplica a todos los actores que en el desempeño de su rol deban publicar información digital en el sitio web del Instituto de Tránsito de Boyacá - ITBOY.

8. OBJETIVO DEL PROCESO DE COMUNICACIÓN

Regular, planear y desarrollar políticas que permitan el control total de los medios, a fin de fortalecer la interrelación en los temas de interés público y la generación de confianza entre los actores.

El plan estratégico de comunicación es integral y que recoge políticas, recursos, procedimientos y acciones a desarrollar a fin de involucrar todos los demás procesos del Instituto de Transito de Boyacá **(ITBOY).**

8.1 Sub-División del Proceso Estratégico de Comunicación

El proceso de comunicación está dividido en 7 actividades bases que lo soportan:

1. **Origen de la información:** Hecho, declaración o anuncio.
2. **Procesamiento:** a través de entrevista o interpretación de un documento oficial.
3. **Redacción:** Construcción de la noticia a partir de la pirámide invertida.
4. **Revisión:** Una vez pirámide invertida. redactada la noticia se revisará para asegurar coherencia e integralidad del texto.
5. **Envío:** Envío del texto definitivo a la Oficina de Comunicaciones ITBOY.
6. **Edición:** El texto se somete a evaluación para verificar el cumplimiento de parámetros.
7. **Publicación:** Envío a la Oficina asesora de Comunicaciones y protocolo de la gobernación de Boyacá, y/o los diferentes medios de comunicación.

Ilustración 4. Subdivisión Proceso Comunicación

Fuente. Instituto de Tránsito de Boyacá **(ITBOY)**.

9. ACTIVOS INFORMÁTICOS

Basados en la metodología de Magerit 3.0, se define activo como “Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.” (MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1 - Método, 2012).

9.1 Determinación de Activos informáticos

Durante el análisis de riesgos para el proceso estratégico de comunicación del Instituto de Transito de Boyacá (ITBOY). Se realizó la identificación de los activos que soportan dicho proceso y a los cuales se agruparon en sub-conjuntos o capas como lo sugiere Magerit 3.0. Para luego determinar a qué

amenazas están expuestos y estimar el impacto que tendría el daño sobre este si la amenaza se materializa.

9.2 Identificación de activos del proceso Comunicación del ITBOY

En el proceso estratégico de comunicación, se identificaron los siguientes activos, los cuales se muestran en la siguiente tabla:

Tabla 2. Activos de información del ITBOY

Categoría de Activos	Cantidad
1. Activos esenciales:	
• Información	4
• Servicios prestados	6
2. Sistemas	
• Comunicaciones	4
• Aplicaciones (Software)	4
• Equipos de Cómputo (Hardware)	4
• Infraestructura Física	2
3. Personal	6
TOTAL	**30**

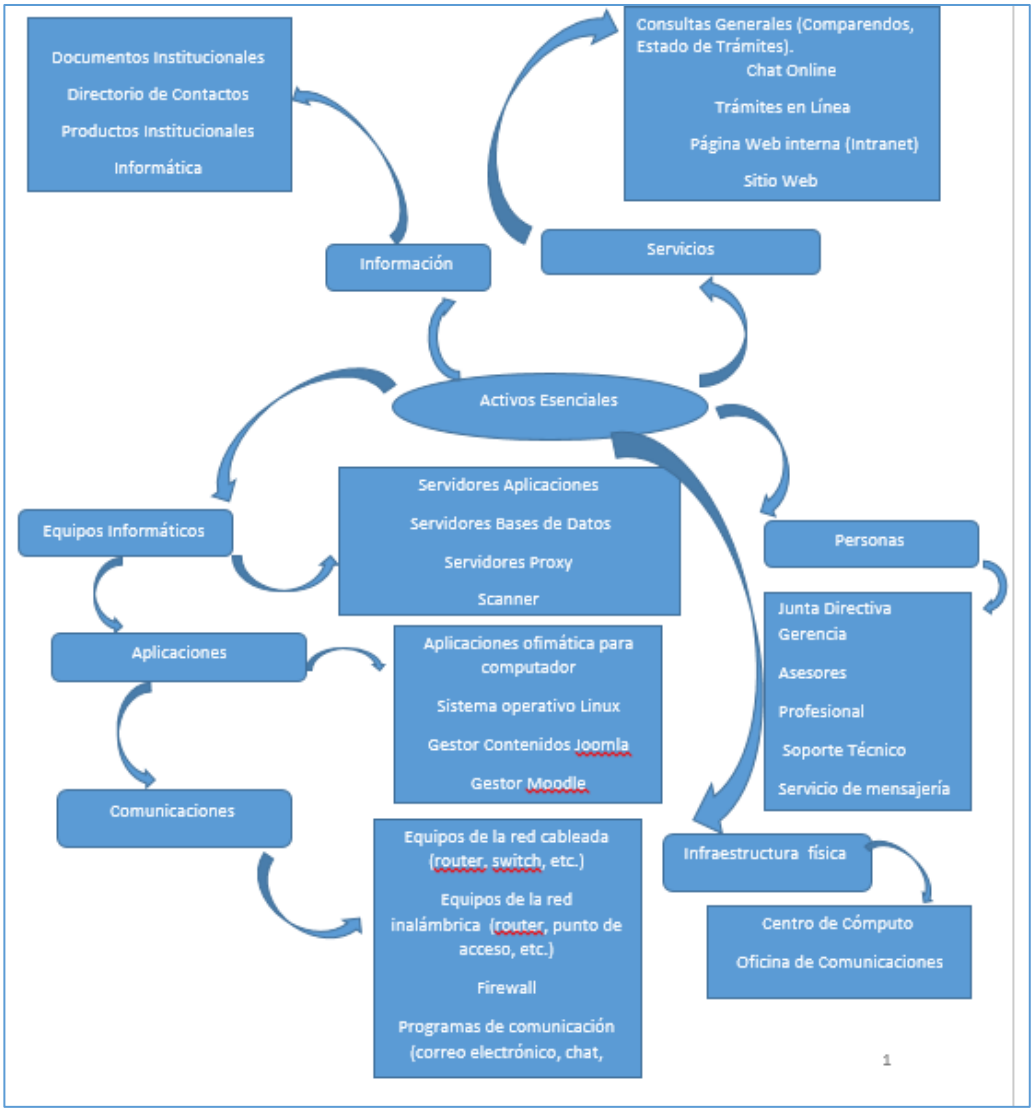
Fuente. Elaboración propia

Se detallan los activos de información del ITBOY ver **Anexo H.**

Dependencia de los activos

En la siguiente figura se describen las dependencias entre los activos identificados; además de mostrar la relación entre los activos esenciales, sistemas y personal.

Ilustración 5. Dependencia de los Activos Informáticos del ITBOY



Fuente. Elaboración Propia

9.3 Valoración de Activos

Aunque asignar valor a un activo es una tarea dispendiosa es necesario hacerlo como lo referencia Magerit 3.0 “Valoración de Activo (coste dinerario requerido para “curar” el activo) y es frecuente la tentación de ponerle precio a todo. Si se consigue, excelente. Incluso es fácil ponerle precio a los aspectos más tangibles (equipamiento, horas de trabajo, etc.); pero al entrar en valoraciones más abstractas (intangibles como la credibilidad de la Organización) la valoración económica exacta puede ser escurridiza y motivo de agrias disputas entre expertos”. (MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1 - Método, 2012).

La valoración de activos de **ITBOY** se realiza de manera cualitativa, ya que al asignarle un valor a la información y a los servicios prestados es subjetivo, puesto que a la fecha el Instituto de Transito de Boyacá **(ITBOY)** no tiene cuantificado estos valores.

Lo primero que se realizara es valorar cada una de las dimensiones de cada activo (Disponibilidad, Integridad y Confidencialidad), lo cual nos permitirá valorar las consecuencias en caso que una amenaza se materialice como lo sugiere Magerit 3.0. Para cada activo y dimensión se determinó una valoración según la escala estándar propuestas por Magerit 3.0.

Tabla 3. Escalas Aplicaciones - Estándar

Escalas Aplicaciones - Estándar
[pi] Información de carácter personal
[lpo] Obligaciones legales
[si] Seguridad
[da] Interrupción del servicio
[olm] Operaciones
[adm] Administración y gestión
[lg] Pérdida de confianza (reputación)
[crm] Persecución de delitos
[rto] Tiempo de recuperación del servicio
[lbl.nat] Información clasificada (nacional)

Fuente. (MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 2 - Catalogo, 2012)

Usando la siguiente escala propuesta por Magerit 3.0 realizaremos la evaluación cualitativa.

Tabla 3. Escala de valoración cualitativa de activos (Impactos)

Valor		Criterio
10-12	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Fuente. (MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 2 - Catalogo, 2012)

9.4 Amenazas

Basados en Magerit 3.0 una amenaza se describe como "Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización" (MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1 - Método, 2012).

Para el Instituto de Transito de Boyacá **(ITBOY),** se identificaron los siguientes grupos de amenazas.

- ON - Origen Natural
- OI - Origen Industrial
- DA - Defecto de Aplicaciones
- FI - Fallas Intencionales
- FA - Fallas Accidentales
- OS - Fallas en la gestión y operación del servicio.

9.4.1 Identificación de amenazas

Para cada activo identificado en el proceso estratégico de Comunicación de **ITBOY,** se realizó el ejercicio de identificar y dar valor a cada una de las amenazas identificada remitirse al **Anexo I.**

9.5 Valoración de amenazas

Probabilidad de Amenaza:

Tabla 4. Valoración de Amenazas**.** Valoración de Amenazas**.** Valoración de Amenazas

Valoración Amenazas	Definición
1	Muy Bajo
2	Bajo
3	Medio
4	Alto
5	Muy Alto

Fuente. Elaboración Propia

Tabla 5. Tabla Calificación Probabilidad

NIVEL DE PROBABILIDAD	DEFINICIÓN DE LA PROBABILIDAD
Alta	La fuente de amenaza es altamente motivada y suficientemente capaz. Los controles para prevenir que la vulnerabilidad suceda son ineficientes.
Media	La fuente de amenaza es motivada y capaz. Los controles pueden impedir el éxito de que la vulnerabilidad suceda.
Baja	La fuente de amenaza carece de motivación. Los controles están listos para prevenir o para impedir significativamente que la vulnerabilidad suceda.

Fuente. Definición de la probabilidad (Sosa, 2012)

Los criterios de aceptación del riesgo son establecidos de forma discrecional por la dirección del Instituto, para tal efecto, se establece una evaluación para ponderar hasta dónde es tolerable y posible su aceptación, este criterio no se valora dependiendo de una alta calificación como se aprecia en la tabla 7 de este documento referente a los activos de información; los criterios de aceptación del riesgo se pueden expresar en términos de beneficios para la organización, de manera concreta para el caso de estudio, el servicio de chat en línea está clasificado como de alto riesgo, sin embargo es aceptable ya que el riesgo de interrupción del servicio puede ser muy alta pero el perjuicio para la entidad es bajo, por cuánto este evento no afecta el cumplimiento de los objetivos estratégicos del ITBOY.

La intranet es un proceso que se encuentra clasificado como alto pues cuenta con un rango de 9 siendo 12 el más alto, sin embargo si bien es cierto la posibilidad de una caída del sistema igualmente y según lo visto por la dirección permite su aceptación por

no afectar un proceso misional de la organización y menos aún al proceso estratégico de comunicaciones.

En conclusión los dos riesgos enunciados son aceptables a pesar de ser calificados como altos, dado que existen otros medios de comunicación tradicionales (correo electrónico, PQRSF, llamadas telefónicas, visita presencial a las oficinas) para continuar atendiendo los requerimientos de los usuarios.

10. INFORME ANÁLISIS DE RIESGOS

Con este análisis se pretende establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto; en la actualidad existen métodos y estándares para el análisis de riesgos; para este caso de estudio se seleccionó Magerit 3.0, ya que implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos del gobierno tomen decisiones, teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Magerit (MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1 - Método, 2012) Persigue los siguientes objetivos:

1. Sensibilizar a los directivos y administradores del Instituto de Transito de Boyacá (ITBOY) de la existencia de riesgos y necesidad de gestionarlos.
2. Entregar un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
3. Descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.
4. preparar a la Organización para procesos de evaluación, auditoría, Certificación o acreditación, según corresponda en cada caso.

En la **Tabla 6.** se analiza los riesgos de los activos de información del objetivo estratégico de comunicación del Instituto de Tránsito de Boyacá **- ITBOY** los cuales son importantes para referenciar su impacto en la institución y su calificación está en el rango de 9 a 12 puntos ver **Anexo I.**

Tabla 6. Análisis de Riesgos del ITBOY

ACTIVO	SUB-ACTIVO	CALIFICACIÓN	ANÁLISIS
Esenciales	Servicio de Consulta Generales (Comparendos, Estado de Tramites).	12	La indisponibilidad del sitio web traumatiza la operatividad del servicio, dado que el módulo de consultas, es la base fundamental que permite a los usuarios verificar los estados de sus trámites(comparendos, certificados de tradición)
Esenciales	Servicio de Tramites en Línea	12	Los resultados arrojados por la matriz evidencian un riesgo muy alto que debe ser atendido, pues se muestra debilidad en la posibilidad de intrusión o infiltración al sistema de información que genera los trámites en línea y la administración del sitio Web.
Esenciales	Sitio Web	12	* Fallas en los sistemas de detección de intrusos afectan la integridad de la información contenida en el sitio web * Falta de compatibilidad entre las aplicaciones y el gestor de contenidos (joomla) por ser software libre. * Publicación irresponsable (sin autorización de la dirección) de artículos que afectan la imagen institucional.
Esenciales	Informática (Planes, Documentación, etc.)	12	El no cumplimiento de las leyes 1712(transparencia), 1474 (anticorrupción) establecen como de obligatorio cumplimiento la publicación de planes, resoluciones, procesos contractuales) acarreará sanciones.
Esenciales	Servicio de Manejo PQRS	12	Las entidades del estado están constantemente monitoreados por los entes de control que exigen medios de comunicación entre los usuarios y la entidad a fin de medir transparencia, así mismo lo exige gobierno en línea.
Esenciales	Servicio de Chat Online	12	El decreto 019 del 2,012 (Antitrámite) establece lineamientos destinados a la orientación y disminución de trámites a los usuarios del estado.
Personal	Junta Directiva	12	Violación de las políticas de seguridad al realizar solicitudes de operación sin el conocimiento necesario.
Personal	Gerencia	12	Violación de las políticas de seguridad al realizar solicitudes de operación sin el conocimiento necesario.
Esenciales	Productos institucionales (Folletos, Fotos, etc.)	9	Pérdida de credibilidad de la ciudadanía por contenido errado de los servicios ofrecidos por el instituto sin garantizar la idoneidad de la información.

Esenciales	Página Web interna (Intranet)	**9**	El mal manejo de la información interna como comunicaciones y mensajes institucionales conllevan a errores en procedimientos y lineamientos establecidos por la dirección.
Sistemas	Equipos de la red cableada (router, switch, etc.)	**9**	La falta de prevención mediante la programación de mantenimiento preventivo y oportunidad en el mantenimiento correctivo generan falas físicas que conllevan a colapsos graves en los sistemas de información
Sistemas	Firewall	**9**	Debilidad en la configuración y desempeño por Obsolescencia
Sistemas	Servidores	**9**	Obsolescencia tecnológica: * Los servidores tiene más de 5 años de uso y no cuentan con soporte director con proveedor. * Los servidores se encuentran conectados a un mismo circuito eléctrico. * Los Servidores se encuentran en un C.C que no está acondicionado para prestar servicios de misión crítica.
Sistemas	Aplicaciones (Software)	**9**	* Los sistemas core de la institución no están configurados en forma redundante (Clúster u HA) permitiendo punto único de fallo. * Al ser software libre tiene defectos en el código produciendo operaciones defectuosas lo que puede alterar la integridad de los datos. * El conocimiento del Software CORE está en manos de personal externo.
Sistemas	Bases de Datos	**9**	No se cuenta con redundancia, lo que evidencia falta de plan de contingencia en caso de daños en los servidores.
Sistemas	Respaldo Datos	**9**	Falta de procedimiento para la custodia de los datos (backup), ya que no existen convenios con otras entidades del estado para salvaguárdalos.
Sistemas	Infraestructura física	**9**	El C.C no cumple con los estándares mínimos para salvaguardar hardware de alta criticidad. El Acceso al centro de cómputo se realiza con restricciones mínimas.
Personal	Asesores	**9**	Malas decisiones por carencia de conocimientos tecnológicos.
Personal	Profesional	**9**	Malas prácticas de los procedimientos especializados.
Personal	Soporte Técnico	**9**	No seguir los procedimientos establecidos para el desarrollo de sus funciones

Fuente. Elaboración propia

CONTROLES Y MITIGACIONES PARA EL PROCESO DE COMUNICACIONES DEL ITBOY

Considerando la definición de riesgo como la amenaza latente de que ocurra un evento, que afecte de manera significativa a la organización, las consecuencias que atentan contra el buen nombre y la operatividad de la misma, se debe entonces tomar acciones que reduzcan la posibilidad de ocurrencia.

En la actualidad las organizaciones y no siendo el ITBOY una excepción, cuentan con sistemas tecnológicos en aras de automatizar los sistemas de información, este proceso será eficiente siempre y cuando la dirección sea consciente de que la administración del riesgo juega un papel crítico; la identificación de los riesgos que puedan afectar los activos de información son fundamentales para aclarar el panorama y vislumbrar posibles acciones que prevengan y si es el caso, mitiguen estos riesgos para minimizar su impacto.

Para nuestro caso de estudio se utilizó los controles indicados en la ISO/IEC 27002:2005, como guía de buenas prácticas permitirá mitigar los riesgos, amenazas y vulnerabilidades del proceso de comunicaciones existentes en el ITBOY, con las medidas, acciones y documentos.

Tabla 7. Controles y Mitigaciones para el ITBOY

ACTIVO	SUB-ACTIVO	CALIFICACIÓN	LITERAL / NOMBRE	DESCRIPCIÓN DEL CONTROL	RESPONSABLE
Esenciales	Servicio Consulta Generales (Comparendos, Estado de Tramites).	12	10. Gestión de Comunicación y Operaciones 10.9 Servicio de Comercio Electrónico 10.9.3 Información Públicamente disponible	Se debería proteger la integridad de la información que pone a disposición en un sistema de acceso público para prevenir modificaciones no autorizadas	Administrador plataforma tecnológica (Profesional Especializado-Sistemas)
Esenciales	Servicio Tramites en Línea	12	10. Gestión de Comunicación y Operaciones 10.9 Servicio de Comercio Electrónico 10.9.2 Transacciones en línea	Se debería proteger la información involucrada en el comercio electrónico que pasa por redes públicas contra actividades fraudulentas, disputas por contratos y divulgación o modificación no autorizadas.	Administrador plataforma tecnológica (Profesional Especializado-Sistemas)
Esenciales	Sitio Web	12	10. Gestión de Comunicación y Operaciones 10.9 Servicio de Comercio Electrónico 10.9.3 Información Públicamente disponible	Se debería proteger la integridad de la información que pone a disposición en un sistema de acceso público para prevenir modificaciones no autorizadas	Administrador plataforma tecnológica (profesional especializado)
Esenciales	Informática (Planes, Documentación, etc.)	12	07. Gestión de Activos 7 2 Clasificación de la Información 7.2.1 Directrices de Clasificación	La información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización.	Administrador plataforma tecnológica Administrador plataforma tecnológica (Profesional Especializado)
			15. Cumplimiento 15.1 Conformidad con los requisitos legales 15.1.3. Salvaguarda de los registros de la Organización	Los registros importantes se deberían proteger de la pérdida, destrucción y falsificación, de acuerdo a los requisitos estatutarios, regulaciones, contractuales y de negocio	Administrador plataforma tecnológica (profesional especializado)

Esenciales	Servicio Manejo PQRS	**12**	10. Gestión de Comunicaciones y Operaciones 10.10 Supervisión 10.10.1. Registros de auditoria	Se deberían producir y mantener durante un periodo establecido los registros de auditoria con la grabación de las actividades de los usuarios, excepciones y eventos de la seguridad de información, con el fin de facilitar las investigaciones futuras y el monitoreo de los controles de acceso.	Administrador plataforma tecnológica (profesional especializado)
Esenciales	Servicio. Chat Online	**12**	10. Gestión de Comunicaciones y Operaciones 10.8 Intercambio de información 10. 8. 4. Mensajería electrónica	Se debería proteger adecuadamente la información contenida en la mensajería electrónica.	Administrador plataforma tecnológica(Profesional especializado-Sistemas)
Personal	Junta Directiva	**12**	08. Seguridad ligada a los Recursos Humanos 8 2 Seguridad en el desempeño de las funciones del empleo 8.2.2. Formación y capacitación en seguridad de la información	Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo	Administrador plataforma tecnológica (profesional especializado)
			08. Seguridad ligada a los Recursos Humanos 8 1 Seguridad en la definición del trabajo y los recursos 8.1.1. Inclusión de la seguridad en las responsabilidades laborales	Se deberían definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización.	Administrador plataforma tecnológica(profesional especializado)
Personal	Gerencia	**12**	06. Organización de la Seguridad de Información 6 1 Organización Interna 6.1.3. Asignación de responsabilidades	Se deberían definir claramente todas las responsabilidades para la seguridad de la información.	Administrador plataforma tecnológica(profesional especializado)

Esenciales	Productos institucionales (Folletos, Fotos, etc.)	**9**	07. Gestión de Activos 7.1 Responsabilidad sobre los activos 7.1. 3 Acuerdos sobre el uso adecuado de los activos	Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.	Administrador plataforma tecnológica (profesional especializado)
Esenciales	Página Web interna (Intranet)	**9**	10. Gestión de Comunicaciones y Operaciones 10 1 Procedimientos y responsabilidades de operación 10.1.2. Control de cambios operacionales	Se deberían controlar los cambios en los sistemas y en los recursos de tratamiento de la información.	Administrador plataforma tecnológica (profesional especializado)
			11. Control de Accesos 11. 2 Gestión de acceso de usuario 11.2.2. Gestión de privilegios	Se debería restringir y controlar la asignación y uso de los privilegios.	Administrador plataforma tecnológica (profesional especializado)
			12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información 12 5 Seguridad en los procesos de desarrollo y soporte 12.5.1. Procedimientos de control de cambios	Se debería controlar la implantación de cambios mediante la aplicación de procedimientos formales de control de cambios.	Administrador plataforma tecnológica (profesional especializado)
Sistemas	Equipos de la red cableada (router, switch, etc.)	**9**	11. Control de Accesos 11.4 Control de acceso en red 11.4.1. Política de uso de los servicios de red	Se debería proveer a los usuarios de los accesos a los servicios para los que han sido expresamente autorizados a utilizar.	Administrador plataforma tecnológica (profesional especializado-Sistemas(
			11. Control de Accesos 11 4 Control de acceso en red 11.4.7. Control de encaminamiento en la red	Se deberían establecer controles de enrutamiento en las redes para asegurar que las conexiones de los ordenadores y flujos de información no incumplen la política de control de	

				accesos a las aplicaciones de negocio.	Administrador plataforma tecnológica
Sistemas	Firewall	**9**	11. Control de Accesos 11 2 Gestión de acceso de usuario 11.2.4. Revisión de los derechos de acceso de los usuarios	El órgano de Dirección debería revisar con regularidad los derechos de acceso de los usuarios, siguiendo un procedimiento formal.	Administrador plataforma tecnológica
			11. Control de Accesos 11 4 Control de acceso en red 11.4.4. Protección a puertos de diagnóstico remoto	Se debería controlar la configuración y el acceso físico y lógico a los puertos de diagnóstico.	Administrador plataforma tecnológica
Sistemas	Servidores	**9**	09. Seguridad Física y del Entorno 9 1 Áreas seguras 9.2.1. Instalación y protección de equipos	El equipo debería situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno, así como las oportunidades de acceso no autorizado.	Administrador plataforma tecnológica
Sistemas	Aplicaciones (Software)	**9**	11. Control de acceso 11.6 Control de acceso a las aplicaciones y a la información. 11.6.1. Restricción de acceso a la información	Se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.	Administrador plataforma tecnológica
Sistemas	Bases de Datos	**9**	15. Cumplimiento 15.1 Conformidad con los requisitos legales 15.1.3. Salvaguarda de los registros de la Organización	Los registros importantes se deberían proteger de la pérdida, destrucción y falsificación, de acuerdo a los requisitos estatutarios, regulaciones, contractuales y de negocio	Administrador plataforma tecnológica
Sistemas	Respaldo Datos	**9**	10. Gestión de Comunicaciones y Operaciones 10.5 Copias de seguridad.	Se deberían hacer regularmente copias de seguridad de toda la información esencial del negocio y del software, de	

			10.5.1 Copias de seguridad de la información.	acuerdo con la política acordada de recuperación.	Administrador plataforma tecnológica
			15. Conformidad 15 1 Conformidad con los requisitos legales 15.1.3. Salvaguarda de los registros de la Organización	Los registros importantes se deberían proteger de la pérdida, destrucción y falsificación, de acuerdo a los requisitos estatutarios, regulaciones, contractuales y de negocio.	Administrador plataforma tecnológica
Sistemas	Infraestructura física	**9**	09. Seguridad Física y del Entorno 9 1 Áreas seguras 9.2.1. Instalación y protección de equipos	El equipo debería situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno, así como las oportunidades de acceso no autorizado.	Administrador plataforma tecnológica
			9. Seguridad física y del entorno 9.2 Seguridad de los equipos 9.2.2. Suministro eléctrico	Se deberían proteger los equipos contra fallos en el suministro de energía u otras anomalías eléctricas en los equipos de apoyo.	Administrador plataforma tecnológica
			9. Seguridad física y del entorno 9.2 Seguridad de los equipos 9.2.4. Mantenimiento de equipos	Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad.	Administrador plataforma tecnológica(profesional especializdo(
Personal	Asesores	**9**	08. Seguridad ligada a los Recursos Humanos 8 2 Seguridad en el desempeño de las funciones del empleo 8.2.3. Procedimiento disciplinario	Debería existir un proceso formal disciplinario para empleados que produzcan brechas en la seguridad.	Administrador plataforma tecnológica
Personal	Profesional	**9**	11. Control de Accesos 11 5 Control de acceso al sistema operativo 11.5.2. Identificación y	Todos los usuarios deberían disponer de un único identificador propio para su uso personal y exclusivo. Se debería elegir una técnica de autenticación adecuada	

			autenticación de usuario	que verifique la identidad reclamada por un usuario.	
Personal	Soporte Técnico	**9**	08. Seguridad ligada a los Recursos Humanos 8 2 Seguridad en el desempeño de las funciones del empleo 8.2.2. Formación y capacitación en seguridad de la información	Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo	Administrador plataforma tecnológica(Profesional especializado-Sistemas)

Fuente. Elaboración propia

11. INDICADORES Y MÉTRICAS

La guía de indicadores de gestión para la Seguridad y Privacidad de la información de MinTIC, se fundamenta en las normas NTC ISO/IEC 27001 e ISO/IEC 27004 vigentes, así como en los anexos con derechos reservados de ISO/ICONTEC, el cual nos sirvió de insumo para este caso de estudio en el proceso estratégico de comunicaciones de ITBOY.

Los indicadores de gestión nos permiten medir la efectividad, eficiencia y eficacia de la ejecución de los procedimientos, clasificados en:

Métricas estratégicas: contemplan la administración del riesgo, objetivos del negocio y cumplimiento (estándares, legislación, auditorías).

Métricas tácticas: contemplan el perímetro (firewall, IDS/IPS, antivirus, anti Spam), aplicaciones (revisión de código fuente, defectos y vulnerabilidades del software), servicios (administración de parches, aseguramiento de equipos, control de cambios).

Métricas Operativas: contemplan la confidencialidad (accesos no autorizados, configuración, por defecto, suplantación de IP o datos), integridad (eliminar, borrar u manipular datos, virus informáticos) y disponibilidad (negación del servicio, inundación de paquetes, eliminación, borrado o manipulación de datos).

Se definieron las siguientes métricas ajustadas al formato sugerido en el documento **Guía de indicadores de gestión Para la seguridad de la información:**

Ilustración 6. Indicador 1

PROCESO: COMUNICACIONES ITBOY					
INDICADOR 01 - CUBRIMIENTO DEL SGSI ITBOY					
DEFINICIÓN					
El indicador permite determinar y hacer seguimiento al cubrimiento de SGIS en ITBOY sobre los riesgos críticos hallados en la entidad y los controles aplicados.					
OBJETIVO					
Hacer seguimiento a la inclusión de nuevos activos críticos de información y su control, dentro del marco de seguridad y privacidad de la información.					
TIPO DE INDICADOR :GESTION					
DESCRIPCION DE LA VARIABLE		FÓRMULA		FUENTE DE INFORMACION	
VA01: Número de activos críticos (Riesgos Muy Altos y Altos) de información incluidos en el alcance de implementación del modelo.		**(VA01/VA02)*100**		Alcance del SGSI, Inventario de Activos de información, plan de tratamiento, matriz de riesgos.	
VA02: Número de activos críticos (Riesgos Muy Altos y Altos) de información incluidos en el alcance de implementación del modelo.				Inventario de Activos de información.	
METAS					
MINIMA	75% - 80%	SATISFACTORIA	80% - 90%	SOBRESALIENTE	100%
OBSERVACIONES					
El indicador de cada proceso debe ser recolectado y promediado para construir un indicador que refleje el estado de ITBOY. El terminó “incluir un activo” debe ser entendido como realizar la correcta clasificación del activo, tratamiento, evaluación de riesgos sobre el mismo y determinación de controles para minimizar el riesgo calculado.					

Fuente. Elaboración propia apoyado de (Ministerio de Tecnologías de la Información y Comunicaciones, s.f.)

Ilustración 7.Indicador 2

PROCESO: COMUNICACIONES ITBOY					
INDICADOR 02 - PLAN SENSIBILIZACIÓN					
DEFINICIÓN					
El indicador permite medir la aplicación de los temas sensibilizados en seguridad de la información por parte de los usuarios finales. Estas mediciones se podrán realizar por medio de auditorías especializadas en el tema o de forma aislada por parte de los responsables de la capacitación y sensibilización.					
OBJETIVO					
El objetivo del indicador es establecer la efectividad de un plan de capacitación y sensibilización previamente definido como medio para el control de incidentes de seguridad.					
TIPO DE INDICADOR :GESTION					
DESCRIPCION DE LA VARIABLE		FÓRMULA		FUENTE DE INFORMACION	
VA01: Número de fallas o no cumplimientos encontrados en las sensibilizaciones programadas o eventos realizados para evaluar el tema.		**(VA01/VA02)*100**		Jeje de Sistemas de Información, auditorías internas, atención al usuario, listas de asistencia	
VA02: Total de personal a capacitar.				Total de funcionarios de la entidad.	
METAS					
MINIMA	75% - 80%	SATISFACTORIA	80% - 90%	SOBRESALIENTE	100%
OBSERVACIONES					
Para el levantamiento de la información que permita obtener datos para la medición el responsable debe idear planes, laboratorios o actividades periódicas que permitan medir lo capacitado o divulgado.					

Fuente. Elaboración propia apoyado de (Ministerio de Tecnologías de la Información y Comunicaciones, s.f.)

Ilustración 8.Indicador 3

PROCESO: COMUNICACIONES ITBOY					
INDICADOR 03 - ATAQUES INFORMATICOS A LA ENTIDAD					
DEFINICIÓN					
Porcentaje de ataques informáticos recibidos en la entidad que impidieron la prestación de alguno de sus servicios.					
OBJETIVO					
Busca conocer el número de ataques informáticos que recibe la entidad y el No. de ataques mitigados.					
TIPO DE INDICADOR : CUMPLIMIENTO					
DESCRIPCION DE LA VARIABLE		FÓRMULA		FUENTE DE INFORMACION	
VA01: No. ataques informáticos que recibió la entidad en el trimestre.		**(VA01/VA02)*100**		Herramientas de Monitoreo/Usuarios Internos.	
VA02: No. ataques informaticos que mitigaron los sistemas de seguridad implementados en la entidad.				Herramientas de Monitoreo/Usuarios Internos.	
METAS					
MINIMA	90% - 95%	SATISFACTORIA	96% - 99%	SOBRESALIENTE	100%
OBSERVACIONES					
Para el levantamiento de la información que permita obtener datos para la medición el responsable debe idear planes, laboratorios o actividades periódicas que permitan medir lo capacitado o divulgado.					

Fuente. Elaboración propia apoyado de (Ministerio de Tecnologías de la Información y Comunicaciones, s.f.)

Ilustración 9. Indicador 4

PROCESO: COMUNICACIONES ITBOY					
INDICADOR 04 - CONTROL DE PUBLICACIONES					
DEFINICIÓN					
Porcentaje de publicaciones cargadas en los S.I de manera exitosa.					
OBJETIVO					
Medir el numero de publicaciones que cumplen con los estandares establecidos en la politica de seguridad.					
TIPO DE INDICADOR : GESTION					
DESCRIPCION DE LA VARIABLE		FÓRMULA		FUENTE DE INFORMACION	
VA01: No. Solicitudes tramitadas.		**(VA01/VA02)*100**		Formato: Control publicaciones pagina WEB	
VA02: No. Solicitudes Recibidas				Formato: Control publicaciones pagina WEB	
METAS					
MINIMA	85% - 90%	SATISFACTORIA	91% - 95%	SOBRESALIENTE	96% - 100%
OBSERVACIONES					
Para el levantamiento de la información que permita obtener datos para la medición el responsable debe basarce en la el formato de Control Publicaciones pagina WEB.					

Fuente. Elaboración propia apoyado de (Ministerio de Tecnologías de la Información y Comunicaciones, s.f.)

Ilustración 10. Indicador 5

PROCESO: COMUNICACIONES ITBOY					
INDICADOR 05 - DISPONIBILIDAD DE LOS SERVICIOS PRESTADOS POR EL PROCESO DE COMUNICACIONES.					
DEFINICIÓN					
Porcentaje de disponibilidad de los servicios que presta el proceso de Comunicaciones de ITBOY.					
OBJETIVO					
Buscar e identificar el nivel de disponibilidad de los servicio y la información prestados por el proceso de Comunicacion de ITBOY.					
TIPO DE INDICADOR : CUMPLIMIENTO					
DESCRIPCION DE LA VARIABLE		FÓRMULA		FUENTE DE INFORMACION	
VA01: La entidad tiene definidos ANS para los servicios publicados en el proceso de Comunicaciones basados en el cumplimiento de Gobierno en linea.		**(VA01-VA02/VA01)*100**		Herramientas de Gestion y Monitoreo ITBOY.	
VA02: Tiempo en el que el servicio no estuvo disponible.				Herramientas de Gestion y Monitoreo ITBOY.	
METAS					
MINIMA	90% - 95%	SATISFACTORIA	96% - 99%	SOBRESALIENTE	100%
OBSERVACIONES					

Fuente. Elaboración propia apoyado de (Ministerio de Tecnologías de la Información y Comunicaciones, s.f.)

Ilustración 11.Indicador 6

PROCESO: COMUNICACIONES ITBOY					
INDICADOR 06 - PORCENTAJE DE IMPLEMENTACIÓN DE CONTROLES					
DEFINICIÓN					
Porcentaje de avance en la implementación de controles de seguridad.					
OBJETIVO					
Busca identificar el grado de avance en la implementación de controles de seguridad en ITBOY.					
TIPO DE INDICADOR : CUMPLIMIENTO					
DESCRIPCION DE LA VARIABLE		FÓRMULA		FUENTE DE INFORMACION	
VA01: Número de Controles Implementados.		**(VA01/VA02)*100**		Plan de tratamiento de riesgos.	
VA02: Número de Controles que se planearon implementar.				Plan de Tratamiento de riesgos.	
METAS					
MINIMA	75% - 80%	SATISFACTORIA	81% - 90%	SOBRESALIENTE	91% - 100%
OBSERVACIONES					

Fuente. Elaboración propia apoyado de (Ministerio de Tecnologías de la Información y Comunicaciones, s.f.)

11.1 Resumen de Indicadores

Los indicadores como instrumentos de medición, evalúan el estado de un sistema de información, para el caso de esta investigación, permiten cuantificar el grado de cumplimiento de las políticas de seguridad implementadas en el Instituto para determinar y establecer el grado de riesgo, basados en estos resultados es posible crear planes de mejora que garanticen la seguridad del proceso de comunicaciones. “No se puede evaluar lo que no se puede medir”, esta definición apoya el trabajo realizado por cuanto se asignan valores a los posibles riesgos para poder medirlos y tener una idea clara de la actual situación de la entidad objeto de estudio.

Ilustración 12.Resumen de Indicadores del proceso de comunicaciones del ITBOY

INDICADOR	TIPO INDICADOR	DEFINICION	ALCANCE	EXP. MATEMATICA	FORMA DE OBTENCION	META	UNIDAD	FRECUENCIA (Periodicidad)
Cubrimiento SGSI ITBOY	Estrategico	El indicador permite determinar y hacer seguimiento al cubrimiento de SGIS en ITBOY sobre los riesgos críticos hallados en la entidad y los controles aplicados.	Hacer seguimiento a la inclusión de nuevos activos críticos de información y su control, dentro del marco de seguridad y privacidad de la información.	$\%Cubrimiento\ SGSI = \frac{VA01}{VA02} * 100$	**VA01:** Número de activos críticos (Riesgos Muy Altos y Altos) de información incluidos en el alcance de implementación del modelo. **VA02:** Número de activos críticos (Riesgos Muy Altos y Altos) de información incluidos en el alcance de implementación del modelo.	80%	(%)	Semestral
Plan Sensibilizacion ITBOY	Gestion	El indicador permite medir la aplicación de los temas sensibilizados en seguridad de la información por parte de los usuarios finales. Estas mediciones se podrán realizar por medio de auditorías especializadas en el tema o de forma aislada por parte de los responsables de la capacitación y sensibilización.	El objetivo del indicador es establecer la efectividad de un plan de capacitación y sensibilización previamente definido como medio para el control de incidentes de seguridad.	$\%Sensibilizacion\ User = \frac{VA01}{VA02} * 100$	**VA01:** Número de fallas o no cumplimientos encontrados en las sensibilizaciones programadas o eventos realizados para evaluar el tema. **VA02:** Total de personal a capacitar.	80%	(%)	Semestral
Ataques Informaticos a la Entidad	Cumplimiento	Porcentaje de ataques informáticos recibidos en la entidad que impidieron la prestación de alguno de sus servicios.	Busca conocer el número de ataques informáticos que recibe la entidad y el No. de ataques mitigados.	$\%Ataques\ Mitigados = \frac{VA01}{VA02} * 100$	**VA01: N**o. ataques informáticos que recibió la entidad en el trimestre. **VA02**: No. ataques informaticos que mitigaron los sistemas de seguridad implementados en la entidad.	96%	(%)	Trimestral
Control Publicaciones	Gestion	Porcentaje de publicaciones cargadas en los S.I de manera exitosa.	Medir el numero de publicaciones que cumplen con los estandares establecidos en la politica de seguridad.	$Control\ Pubicaciones = \frac{VA01}{VA02} * 100$	**VA01**: No. Solicitudes tramitadas. **VA02:** No. Solicitudes Recibidas	91%	(%)	Trimestral
Disponibilidad de los Servicios Prestados por el proceso de Comunicaciones.	Cumplimiento	Porcentaje de disponibilidad de los servicios que presta el proceso de Comunicaciones de ITBOY.	Buscar e identificar el nivel de disponibilidad de los servicio y la información prestados por el proceso de Comunicacion de ITBOY.	$Disponibilidad = \frac{VA01 - VA02}{VA02} * 100$	**VA01:** La entidad tiene definidos ANS para los servicios publicados en el proceso de Comunicaciones basados en el cumplimiento de Gobierno en linea. **VA02**: Tiempo en el que el servicio no estuvo disponible.	96%	(%)	Mensual
Implementacion de Controles	Cumplimiento	Porcentaje de avance en la implementación de controles de seguridad.	Busca identificar el grado de avance en la implementación de controles de seguridad en ITBOY.	$Impl.Controles = \frac{VA01}{VA02} * 100$	**VA01:** Número de Controles Implementados. **VA02:** Número de Controles que se planearon implementar.	81%	(%)	Trimestral

Fuente. Elaboración propia

12. JUSTIFICACIÓN SGSI ANTE LA GERENCIA

Se identificaron amenazas y riesgos a los activos informáticos, para lo cual se ha creado un documento dirigido Junta Directiva del instituto, el cual contiene recomendaciones y acciones que se consideran deben formar parte integral de la estrategia del proceso de comunicaciones de la Organización que generan disminución y control de los riesgo de la institución.

Este análisis propone cualificar y cuantificar métricas e indicadores, que tienen como objetivo lograr que el Sistema de seguridad de la información en la institución, cumpla con los requisitos definidos por las políticas, normas técnicas y estándares internacionales de seguridad recomendadas y definidas en la política general de Seguridad de la información de ITBOY. Las medidas preventivas y correctivas propuestas forman parte de los estándares de gestión de la seguridad de la información; de esta manera fortalecen y brindan eficacia a las medidas de control actuales, lo que permitirá garantizar la reducción de pérdidas económicas y la continuidad de los servicios brindados por el área de comunicaciones del Instituto de Transito de Boyacá **(ITBOY).**

Para finalizar se enfatiza la gestión de la seguridad de la información es una estrategia, que por medio de indicadores, métricas, procedimientos y políticas permite identificar fallas (Estratégicas, Operativas y tácticas) al interior de la organización y sobre las tecnologías de información como lo asegura (MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1 - Método, 2012) “La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad”.

13. VALORACIÓN DE INCIDENTES

13.1 Análisis de Costos

Los incidentes de seguridad informático, es ineludible desarrollar mecanismos para gestionarlos. Para dar inicio al análisis y valoración de los incidentes de seguridad se debe partir con entender las siguientes definiciones:

- **Costo directo**. corresponde al desembolso directo de gastos para llevar a cabo una determinada actividad.
- **Costos indirectos**. equivale a la cantidad de tiempo, esfuerzo y otros recursos de la organización incurridos, pero sin que estos impliquen un gasto efectivo.
- **El Costo de oportunidad.** es el costo resultante de la pérdida de oportunidades comerciales, como consecuencia de efectos negativos en la reputación, como resultado del de la demora en informar a los clientes víctimas y públicamente a través de los medios de comunicación.
- **Costos Externos:** incluyendo la pérdida de activos de información, interrupción del negocio, daños en el equipo Y la pérdida de ingresos, se capturaron utilizando métodos de costos sombra. Los costes totales se asignaron a Nueve vectores de ataque discernibles: virus, gusanos, troyanos; Malware; Botnets; Ataques basados en la web; Phishing e ingeniería social; Miembros maliciosos; Dispositivos robados o dañados; código malicioso (Incluida la inyección de SQL); Y negación de servicios
- **Centros de Costo:** Los centros de costos identifican cada una de las posibles fases que se deben tener en cuenta para determinar valores en la atención de incidentes de seguridad de la información según el modelo Ponemon Tomado de (Ponemon Org., 2016).

Para estimar el valor de los costos asociados a los incidentes más frecuentes, se investigaron valores de referencia de estudios realizados por las firmas Kaspersky Lab y Ponemon Institute, donde basados en encuestas realizadas a (237) empresas en 6 países, las cuales tuvieron incidentes de seguridad, se pudo obtener valores promedio que sirven de referencia para estimar el costo promedio de los incidentes para una empresas de gran tamaño.

Tabla 8. Análisis Interno de Costos según Kaspersky Lab y Ponemon Institute

ANÁLISIS INTERNO	TIPO DE COSTO	DESCRIPCIÓN	VALOR
Detección (Causas, víctimas probables)	Directo	Presupuesto para actividades forenses y de investigación, servicios de evaluación y auditoría, gestión de equipo de crisis. Adicionalmente se incluyen costos por Valor de la propiedad intelectual, listas de clientes, secretos comerciales, u otros activos que fueron afectados	$ 27,542
Investigación & Escalamiento (Organizar el equipo de Respuesta)	Directo	Contratación de consultores, expertos en gestión de riesgos, abogados, consultores de seguridad físicos y especialistas en relaciones públicas	$ 10,875
Contención (Ataque y Solución al Incidente)	Directo	Actividades que se centran en detener o disminuir el Incidente	Depende de la cantidad de Recursos Físicos y Humanos requeridos para la mitigación.
Recuperación (Puesta en Marcha Sistemas Afectados)	Directo	Actividades asociadas con la reparación y reparación de los sistemas de la organización Y los procesos centrales de negocio. Estos incluyen la restauración de los activos de información dañados	$ 392,984
Respuesta a Post-Incidente (Actividades para que no Vuelva a ocurrir el Incidente).	Indirecto	Actividades para ayudar a la organización a minimizar posibles ataques futuros. Estas Incluir los costos derivados de la interrupción del negocio y la pérdida de información, así como Tecnologías y sistemas de control. Mitigación de Secuelas.	$ 118,780
Valor Total Incidentes en un Año.			**$ 550,181**

Fuente: Elaboración Propia

Tabla 9. Análisis Externo de Costos según Kaspersky Lab y Ponemon Institute

ANÁLISIS EXTERNO	TIPO DE COSTO	DESCRIPCIÓN	VALOR
Perdida de Información	Directo	Pérdida o robo de información sensible y confidencial como Resultado de un ataque cibernético.	Depende de la Sensibilidad de la Información
Disrupción del Negocio	De Oportunidad	El impacto económico del tiempo de inactividad o interrupciones.	$ 105,800.00
Daños en equipos	Directo	Valores ocasionados por la reparación de los equipos afectados por incidentes de seguridad.	$ 566,000.00
Pérdida de Ingresos	Indirecto	Valores asociados o que deja de recibir la compañía por comportamientos anormales de las ventas con clientes, costos asociados por las estrategias de captación de clientes, pérdida de reputación o pérdida del conocimiento del buen hacer.	$ 3,030,814
Valor Total de Incidentes en un Año			**$ 3,702,614.00**

Fuente. Elaboración propia

El laboratorio Kaspersky junto con la empresa B2B international desarrollaron un estudio a más de 4.000 representantes de empresas de 25 países, revisando complejidad de infraestructura, presupuesto y soluciones de seguridad; permitiendo determinar cuánto invierten las empresas tanto para protegerse como para recuperarse después de un incidente de seguridad.

El análisis de costos de los incidentes de seguridad desarrollado según Kaspersky y bajo la metodología de Ponemon, establece información relevante que permite evaluar los costos generados al cristalizarse un riesgo ya previsto en la identificación de incidentes, esta valoración permite establecer criticidad para priorizar las medidas de mitigación de los mismos, a efectos de vislumbrar un horizonte real e un panorama de riesgos que pueden afectar de manera importante la operatividad de la organización.

En términos generales la cuantificación de estos valores, permite a la alta dirección ratificar que la inversión realizada para dar solución de incidentes

hubiese sido mayor de no contemplar estos componentes y analizado el costo de pérdidas por riesgos materializados.

Los costos internos resultados de este análisis indican que las mayores inversiones se realizan en actividades asociadas a la reparación reconstrucción y restauración ocasionada por la afectación a los activos fijos de siendo estos costos directos, que debe contemplarse en la elaboración del presupuesto asignado para la mitigación de los riesgos.

La pérdida de ingresos referente a los costos indirectos (Valores asociados o que deja de recibir la compañía por comportamientos anormales de las ventas con clientes, costos asociados por las estrategias de captación de clientes, pérdida de reputación o pérdida del conocimiento del buen hacer); son los más críticos toda vez que dejan de percibirse recursos importantes sin mencionar la imagen negativa hacia el cliente.

No deben subestimarse los costos que genera la inactividad, interrupción de las operaciones y recuperación de los equipos en el análisis externo (costo de oportunidad); ya que no controlar estos aspectos, puede afectar en el tiempo las finanzas de la organización.

14. CASO DE ESTUDIO INCIDENTES DE SEGURIDAD EN ITBOY

Tabla 10. Análisis Interno y Externo Incidente No.1

ANÁLISIS INTERNO	INCIDENTE	TIPO DE COSTO	TIEMPO (HORAS)	VALOR	VALOR TOTAL
Detección (Causas, víctimas probables) - Virus y malware causan pérdida de productividad	Virus y malware causan pérdida de productividad	Directo	4	$ 61,952	$ 247,808
Investigación & Escalamiento (Organizar el equipo de Respuesta)	Virus y malware causan pérdida de productividad	Indirecto	2	$ -	$ -
Recuperación (Puesta en Marcha Sistemas Afectados)	Virus y malware causan pérdida de productividad	Directo	2	$ 27,542	$ 123,904
Respuesta a Post-Incidente (Actividades para que no Vuelva a ocurrir el Incidente).	Virus y malware causan pérdida de productividad	Directo	2	$ 27,542	$ 123,904
Notificación (Plan de comunicaciones, divulgación)	Virus y malware causan pérdida de productividad	Directo	2	$ 27,542	$ 123,904
Valor Total Incidentes en un Año.			**12**	**$ 144,578**	**$ 619,520**

ANÁLISIS EXTERNO	INCIDENTE	TIPO DE COSTO	TIEMPO (HORA)	VALOR	VALOR TOTAL
Pérdida de Información	Virus y malware causan pérdida de productividad	Directo	4	$ 78,914.00	$ 315,656.00
Disrupción del Negocio	Virus y malware causan pérdida de productividad	Directo	8	$ 104,730.00	$ 837,840.00
Daños en equipos	Virus y malware causan pérdida de productividad	Directo	24	$ 104,730.00	$ 2,513,520.00
Pérdida de Ingresos	Virus y malware causan pérdida de productividad	Directo	4	$ 78,914.00	$ 315,656.00
Valor Total de Incidentes en un Año			**40**	**$ 288,374.00**	**$ 3,667,016.00**

Fuente. Elaboración propia

Tabla 11. Análisis Interno y Externo Incidente No.2

ANÁLISIS INTERNO	INCIDENTE	TIPO DE COSTO	TIEMPO (HORAS)	VALOR	VALOR TOTAL
Detección (Causas, víctimas probables) - Virus y malware causan pérdida de productividad	Uso inapropiado del recurso por los empleados	Indirecto	2	$ 61,952	$ 123,904
(Organizar el equipo de Respuesta)	Uso inapropiado del recurso por los empleados	Indirecto	1	$ 30,976	$ 30,976
Recuperación (Puesta en Marcha Sistemas Afectados)	Uso inapropiado del recurso por los empleados	Indirecto	2	$ 27,542	$ 55,084
Respuesta a Post-Incidente (Actividades para que no Vuelva a ocurrir el Incidente).	Uso inapropiado del recurso por los empleados	Indirecto	4	$ 27,542	$ 110,168
Notificación (Plan de comunicaciones, divulgación)	Uso inapropiado del recurso por los empleados	Indirecto	1	$ 27,542	$ 27,542
Valor Total Incidentes en un Año.			**10**	**$ 175,554**	**$ 347,674**

Análisis Externo	Incidente	Tipo de Costo	Tiempo (horas)	Valor	Valor Total
Pérdida de Información	Uso inapropiado del recurso por los empleados	Indirecto	8	$ 78,914.00	$ 631,312.00
Disrupción del Negocio	Uso inapropiado del recurso por los empleados	Indirecto	2	$ 104,730.00	$ 209,460.00
Daños en equipos	Uso inapropiado del recurso por los empleados	Indirecto	2	$ 104,730.00	$ 209,460.00
Pérdida de Ingresos	Uso inapropiado del recurso por los empleados	N/A			$ -
Valor Total de Incidentes en un Año			**12**	**$ 209,460.00**	**$ 418,920.00**

Fuente. Elaboración Propia

Tabla 12. Análisis Interno y Externo Incidente No.3

ANÁLISIS INTERNO	INCIDENTE	TIPO DE COSTO	TIEMPO (HORAS)	VALOR	VALOR TOTAL

Detección (Causas, víctimas probables) - Virus y malware causan pérdida de productividad	Pérdida física de dispositivos o medios que contengan datos	Directo	8	$ 72,806	$ 582,448
Investigación & Escalamiento (Organizar el equipo de Respuesta)	Pérdida física de dispositivos o medios que contengan datos	Directo	6	$ 72,806	$ 436,836
Recuperación (Puesta en Marcha Sistemas Afectados)	Pérdida física de dispositivos o medios que contengan datos	Directo	2	$ 27,542	$ 55,084
Respuesta a Post-Incidente (Actividades para que no Vuelva a ocurrir el Incidente).	Pérdida física de dispositivos o medios que contengan datos	Directo	2	$ 72,806	$ 145,612
Notificación (Plan de comunicaciones, divulgación)	Pérdida física de dispositivos móviles que exponen riesgo a la organización	Directo	1	$ 72,806	$ 72,806
Valor Total Incidentes en un Año.			**19**	**$ 318,766**	**$ 1,292,786**

ANÁLISIS EXTERNO	INCIDENTE	TIPO DE COSTO	TIEMPO (HORAS)	VALOR	VALOR TOTAL
Pérdida de Información	Pérdida física de dispositivos o medios que contengan datos	Indirecto	1	$ 72,806	$ 72,806.00
Disruption del Negocio	Pérdida física de dispositivos o medios que contengan datos	N/A			$ -
Daños en equipos	Pérdida física de dispositivos o medios que contengan datos	Directo	2	$ 72,806	$145,612.00
Pérdida de Ingresos	Pérdida física de dispositivos o medios que contengan datos	N/A			$ -
Valor Total de Incidentes en un Año			**3**	**$ 72,806.00**	**$145,612.00**

Fuente. Elaboración Propia

Tabla 13. Análisis Interno y Externo Incidente No.4

ANÁLISIS INTERNO	INCIDENTE	TIPO DE COSTO	TIEMPO (HORAS)	VALOR	VALOR TOTAL

Detección (Causas, víctimas probables) - Virus y malware causan pérdida de productividad	Pérdida física de dispositivos móviles que exponen riesgo a la organización	Directo	1	$ 72,806	$ 72,806
Investigación & Escalamiento (Organizar el equipo de Respuesta)	Pérdida física de dispositivos móviles que exponen riesgo a la organización	Directo	1	$ 72,806	$ 72,806
Recuperación (Puesta en Marcha Sistemas Afectados)	Pérdida física de dispositivos móviles que exponen riesgo a la organización	Directo	1	$ 72,806	$ 72,806
Respuesta a Post-Incidente (Actividades para que no Vuelva a ocurrir el Incidente).	Pérdida física de dispositivos móviles que exponen riesgo a la organización	Directo	1	$ 72,806	$ 72,806
Notificación (Plan de comunicaciones, divulgación)	Pérdida física de dispositivos móviles que exponen riesgo a la organización	Directo	1	$ 72,806	$ 72,806
Valor Total Incidentes en un Año.			**5**	**$ 364,030**	**$ 364,030**

ANÁLISIS EXTERNO	INCIDENTE	TIPO DE COSTO	TIEMPO(HORS)	VALOR	VALOR TOTAL
Pérdida de Información	Pérdida física de dispositivos móviles que exponen riesgo a la organización	Indirecto	0.5	$ 72,806	$ 36,403
Disrupción del Negocio	Pérdida física de dispositivos móviles que exponen riesgo a la organización	N/A			$ -
Daños en equipos	Pérdida física de dispositivos móviles que exponen riesgo a la organización	Directo	2	$ 72,806	$ 145,612
Pérdida de Ingresos	Pérdida física de dispositivos móviles que exponen riesgo a la organización	N/A			$ -
Valor Total de Incidentes en un Año			**2.5**	**$145,612.00**	**$182,015.00**

Fuente. Elaboración Propia

Tabla 14. Análisis Interno y Externo Incidente No.5

ANÁLISIS INTERNO	INCIDENTE	TIPO DE COSTO	TIEMPO (HORAS)	VALOR	VALOR TOTAL
Detección (Causas, víctimas probables) - Virus y malware causan pérdida de productividad	Uso inadecuado de datos mediante dispositivos móviles.	Directo	2	$ 72,806	$ 145,612

Investigación & Escalamiento (Organizar el equipo de Respuesta)	Uso inadecuado de datos mediante dispositivos móviles.	Directo	2	$ 72,806	$ 145,612
Recuperación (Puesta en Marcha Sistemas Afectados)	Uso inadecuado de datos mediante dispositivos móviles.	Directo	0.5	$ 72,806	$ 36,403
Respuesta a Post-Incidente (Actividades para que no Vuelva a ocurrir el Incidente).	Uso inadecuado de datos mediante dispositivos móviles.	Directo	0.5	$ 72,806	$ 36,403
Notificación (Plan de comunicaciones, divulgación)	Uso inadecuado de datos mediante dispositivos móviles.	Directo	1	$ 72,806	$ 72,806
Valor Total Incidentes en un Año.			**6**	**$ 364,030**	**$ 436,836**

ANÁLISIS EXTERNO	INCIDENTE	TIPO DE COSTO	TIEMPO (HORAS)	VALOR	VALOR TOTAL
Pérdida de Información	Uso inadecuado de datos mediante dispositivos móviles.	Indirecto			0
Disrupción del Negocio	Uso inadecuado de datos mediante dispositivos móviles.	N/A			0
Daños en equipos	Uso inadecuado de datos mediante dispositivos móviles.	N/A			0
Pérdida de Ingresos	Uso inadecuado de datos mediante dispositivos móviles.	N/A			0
Valor Total de Incidentes en un Año			**0**	**$ -**	**$ -**

Fuente. Elaboración propia

14.1 Análisis de Costos Caso de Estudio ITBOY

Para nuestro caso de estudio referente a los costos de incidentes de seguridad más frecuentes en el Instituto de Transito de Boyacá -ITBOY y apoyándonos con los resultados del estudio del laboratorio Kaspersky; se tomaron como referencia cinco (5) incidentes: Pérdida de Información, disrupción de negocio, daños en equipos y pérdida de ingresos (incidente externo, costo directo); evidenciándose la necesidad de provisionar recursos para atender los posibles costos generados por infecciones informáticas por virus y malware que traumatizan las operaciones en la entidad.

En orden de costos, se aprecian valores ocasionados por la pérdida física de dispositivos o medios que contengan datos, estos costos directos hacen parte de incidentes internos y como bien sabido es, la información es considerada como el activo más valioso de toda organización, no deben entonces escatimarse recursos encaminados a proteger los datos, el análisis indica que igualmente inversiones importantes en la etapa de recuperación deben ser tenidos en cuenta.

Los virus informáticos y los malware son definitivamente como se observa en el cuadro de costos a los que más importancia hay que darle tanto como incidente interno como externo, pues sus constantes ataques ponen en riesgo los sistemas de información de la entidad y contrarrestar los efectos ocasionados representa valores considerables para la entidad.

Las gráficas antes relacionadas reflejan el comportamiento de los incidentes más frecuentes vs los costos de recuperación, de manera concordante con los análisis realizados en el transcurso de este capítulo se concluye la necesidad de prestar toda la atención a la protección de los datos, que son propensos de manera permanente a infecciones informáticas , de prosperar y hacerse efectivo un riesgo de este tipo, los costos en los que incurren las entidades son importantes, más si se tiene en cuenta el papel que juega las probabilidades, no siempre es posible alcanzar una recuperación total logrando desestabilizar a la organización.

Un efecto domino genera reacción sobre la disponibilidad, ocasionando pérdida de productividad e interrupción en la prestación de los servicios que lesiona seriamente la imagen y los ingresos productos de su deber ser.

El factor tiempo es determinante y uno de los actores más importantes en el cálculo de costos por la cristalización de los riesgos, “a mayor tiempo mayor pérdida”, esto lleva a sensibilizar y concientizar a la dirección a fin de enfocar esfuerzos para que en caso de prosperar y hacerse realidad un riesgo, pueda resolverse el impase en el menor tiempo posible.

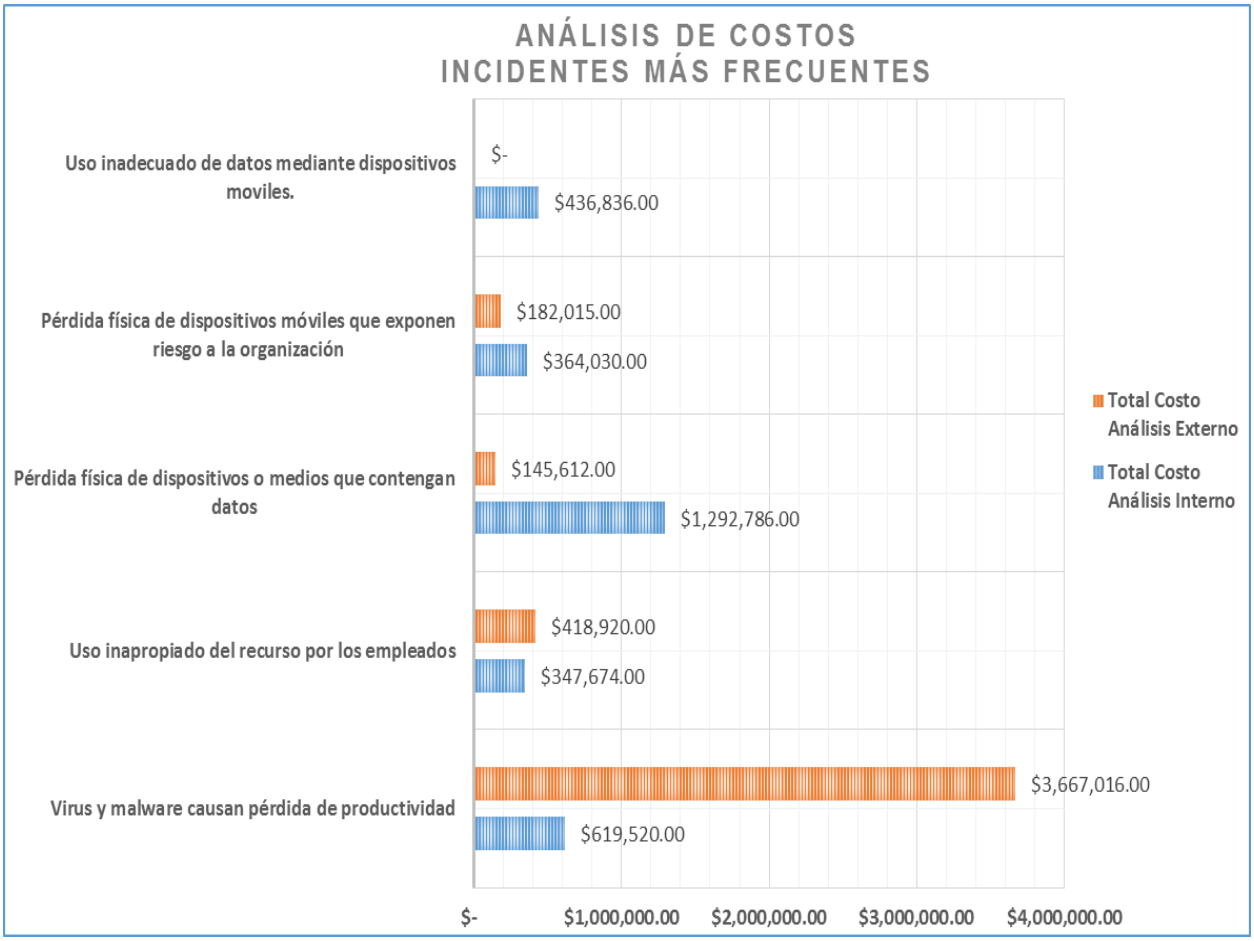
14.2 Análisis Graficas Tiempos y Costos ITBOY

La **Ilustración 15** y la **Ilustración 16,** reflejan el comportamiento de los incidentes más frecuentes Vs los costos de recuperación, de manera concordante con los análisis realizados en el transcurso de este capítulo se concluye la necesidad de prestar toda la atención a la protección de los datos, que son propensos de manera permanente a infecciones informáticas, de prosperar y hacerse efectivo un riesgo de este tipo, los costos en los que incurren las entidades son importantes, más si se tiene en cuenta el papel que juega las probabilidades, no siempre es posible alcanzar una recuperación total logrando desestabilizar a la organización.

Un efecto domino genera reacción sobre la disponibilidad, ocasionando pérdida de productividad e interrupción en la prestación de los servicios que lesiona seriamente la imagen y los ingresos productos de su deber ser.

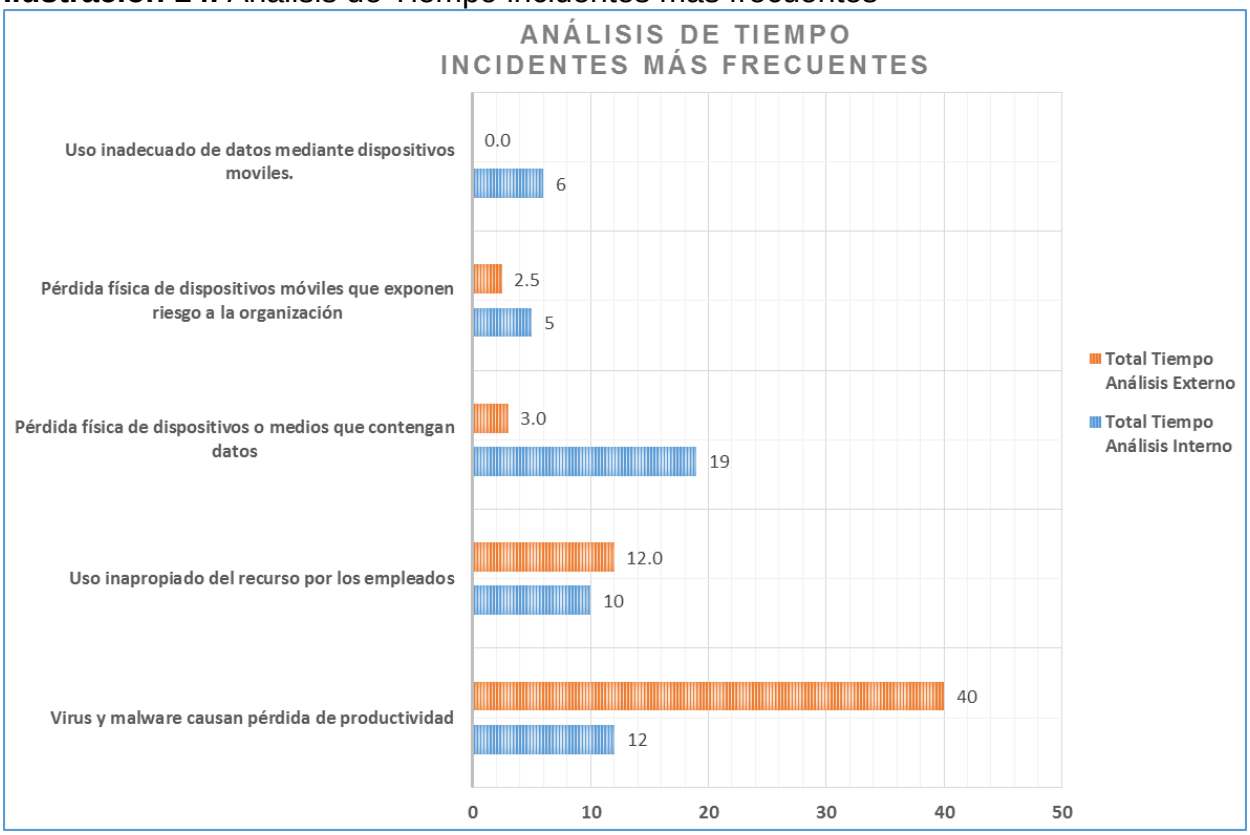
El factor tiempo es determinante y uno de los actores más importantes en el cálculo de costos por la cristalización de los riesgos, “a mayor tiempo mayor pérdida”, esto lleva a sensibilizar y concientizar a la dirección a fin de enfocar esfuerzos para que en caso de prosperar y hacerse realidad un riesgo, pueda resolverse el impase en el menor tiempo posible.

Ilustración 13. Análisis Costos Incidentes más Frecuentes ITBOY



Fuente. Elaboración Propia

Ilustración 14. Análisis de Tiempo incidentes más frecuentes



Fuente. Elaboración Propia

15. Análisis de incertidumbre para el ITBOY

Herramienta: **VENTANA DE AREM.**

La ventana de AREM como la define Cano, J (2013). Es una herramienta cuyo propósito es ampliar la capacidad y el conocimiento del entorno; de forma que se facilite la toma de decisiones basadas sobre las oportunidades y retos empresariales del mundo de hoy, buscando ajustar la práctica actual de la administración de riesgos en un mundo dominado por la tecnología, más aún cuando a ésta se le integran las soluciones de Cloud, los dispositivos móviles, IOT y por último la Big data.

Para nuestro caso de estudio en el ITBOY, ubicamos las amenazas y los riesgos conocidos (área libre), tanto del entorno como del Instituto, todos aquellos que afecten el cumplimiento habitual de las actividades.

Las amenazas y riesgos Focalizados (área oculta), que impactan al Instituto, se ubican las acciones que están inmersas en las actividades web como son las

consultas, trámites en línea, violación de políticas que pueden afectar el funcionamiento del core del negocio en el ITBOY.

Por otra parte se encuentran las amenazas y riesgos latentes (área ciega), en este segmento se ubica todo los riesgos latentes para lo que la entidad no se encuentra preparada, ni controla dichos riesgos y amenazas, para asumir el impacto de una manera preventiva; como son la pérdida de datos confidenciales causados por vulnerabilidades externas, ataques de denegación de servicios a la organización.

Para terminar, están las amenazas y riesgos emergentes (área desconocida), los cuales son riesgos desconocidos en todas las dimensiones (entorno y organización), situaciones que pueden ser posibles consecuencias de la integración de los servicios digitales; y para dónde tiende la globalización con el surgimiento de tecnologías convergentes como son: Grandes datos y analítica, Redes sociales, computación móvil, computación en la nube e Internet de las cosas.

Para Instituto de Tránsito de Boyacá – ITBOY, las aplicaciones principales que gestiona el área de tecnologías producto del proceso estratégico de comunicación, el cual es nuestro objeto de estudio, a continuación se detalla la tecnología más importante que se usa para dicho proceso, dada la importancia de mantener la confiabilidad, integridad, disponibilidad y la confidencialidad de la información:

- Aplicación de Trámites en línea: Los usuarios pueden realizar pagos en línea de comparendos
- Servicio de Consulta Generales: Permite realizar consultas de Comparendos, Estado de Tramites, certificados de tradición de automotores.
- Servicio de PQRS: Se gestiona las diferentes inquietudes de los clientes.
- Redes sociales: Permite un contacto masivo de una manera digital con los usuarios del servicio de consultas generales e la retroalimentación de

Tabla 15. Ventana de AREM

VENTANA DE AREM	LO QUE CONOCE LA ORGANIZACIÓN	LO QUE DESCONOCE LA ORGANIZACIÓN
	RIESGOS CONOCIDOS	**RIESGOS LATENTES**
Lo que conoce el entorno	• Errores de los usuarios • Intrusión de software malicioso • Ataques de virus • Ataques al sitio web • Debilidad en la posibilidad de intrusión o infiltración al sistema de información que genera los trámites en línea y la administración del sitio Web. • Sanciones legales (Leyes 1474, 1712, decreto 019 de 2.012) • Errores de los usuarios (internos y/o externos) • Pérdida de imagen institucional, por contenido errado de los servicios ofrecidos por el instituto sin garantizar la idoneidad de la información. • Acceso no autorizado • Errores en la administración y mantenimiento.	• Ciber Terrorismo • Delincuencia organizada • Pérdida de datos confidenciales causada por vulnerabilidades externas. • Destrucción de la infraestructura digital como de la física y pérdidas humanas. • Denegación de servicios
	RIESGOS FOCALIZADOS	**RIESGOS EMERGENTES**
Lo que desconoce el entorno	• Servicio de Consulta Generales (Comparendos, Estado de Tramites). • Violación de las políticas de seguridad al realizar solicitudes de operación sin el conocimiento necesario • Servicio de Tramites en línea (Aplicaciones Baja en Seguridad). • Falta de compatibilidad entre las aplicaciones y el gestor de contenidos (Joomla) por ser software libre. • Obsolescencia plataforma tecnológica. • No se cuenta con redundancia en los S.I, lo que evidencia falta de plan de contingencia en caso de daños.	• Redes Sociales. • IOT • Potenciación del ciudadano digital. • Impacto de los avances tecnológicos. en el Gobierno. • Ingeniería social. • Riesgos en el manejo del volumen de la información por proliferación de datos. • Derecho a ser olvidado. • Ciber Conflictos. • Incrementos de “botnets” • Conectividad – Movilidad • Manipulación de los significados de la información digital.

Fuente. Elaboración propia apoyada en (Cano J. J., 2014)

16. CONCLUSIONES

Para dar solución a los incidentes, es importante concentrarse en las detecciones y en cómo se está protegiendo la información en las empresas, definiendo estrategias, realizando monitoreo, gestión permanente de los incidentes y protegiendo los activos informáticos críticos.

Los indicadores de gestión y cumplimiento, permiten la mejora continua al evaluar la efectividad, eficiencia y eficacia del modelo de Seguridad y privacidad de la información; los cuales ayudarán al plan establecido para el análisis y tratamiento de riesgo de la organización.

De igual forma con las métricas se logra cuantificar (números o porcentajes), aspectos como cobertura, política interna, perfil o roles, seguridad en el tiempo, éstas se encuentran alineadas con los objetivos de seguridad trazados por la organización. También son las encargadas de medir el desempeño de los controles establecidos; dichos controles unos pueden ser automatizados y disminuyen la operatividad y otros necesariamente se deben comprobar de manera manual y deben tener responsable.

De igual forma el diseñar, analizar y comunicar métricas y controles de la gestión de seguridad de la información en el ITBOY, permitirá desarrollar habilidades para participar en la toma de decisiones con la alta gerencia, que motiven a todos los niveles de empleados a proteger la información.

Por otra parte la globalización, penetración de intrusos informáticos, sofisticación de las ciberamenazas a las empresas hace conveniente, crear para la gestión de incidentes de seguridad informática, un grupo de profesionales encargados CERT (Computer Emergency Response Team) / CSIRT Computer Security Incident Response Team), que ayude a mitigar con rapidez e impacto mínimo, los riesgos a los activos informáticos, en los diferentes ambientes tanto producción como de soporte.

Las lecciones aprendidas referentes al entorno y a la organización permitió proponer a la junta directiva la implementación del SGSI, para el ITBOY.

El resultado de este ejercicio académico, nos permite concluir que las herramientas utilizadas por el ITBOY (Sistema de Detección de Intrusos SDI, Sistema de

Prevención de Intrusos IPS y Proxy) no son suficientes; toda vez que el producto de esta investigación pone al descubierto graves debilidades como es el caso de trámites y consultas en línea a través de la página web del Instituto; que deben ser atendidas a fin de robustecer el sistema de gestión de la seguridad de la información y reducir los de riesgos a los que está expuesta la entidad en el proceso de comunicación.

Para la Dirección será mucho más eficiente y eficaz, la toma de decisiones basadas en instrumentos como los expuestos a lo largo de este trabajo (análisis de activos, políticas de seguridad, matriz de riesgos, indicadores, controles, métricas y análisis de riesgos emergentes); ya que orientan y sensibilizan a todos los niveles de la organización para concientizarse y capacitarlos, y de esta forma se involucren con los procesos de aseguramiento de la información.

BIBLIOGRAFÍA

Archivo General de la Nación. (11 de Septiembre de 2012). *www.archivogeneral.gov.co.* Obtenido de http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/CIRCULAR_05_DE_2012.pdf

Archivo General de la Nacion. (Mayo de 2016). *Archivo General de la Nacion*. Obtenido de http://www.archivogeneral.gov.co/politicas

Cano, J. (2013). *Inseguridad de la Información. Una visión estratégica.* España: Alfaomega.

Congreso de la República. (10 de enero de 2012). *www.alcaldiabogota.gov.co.* Obtenido de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=45322

Congreso de la República. (06 de Marzo de 2014). *alcaldiabogota.gov.co.* Obtenido de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882

Icetex. (2014). *Instituto Colombiano de Extudios en el Exterior*. Obtenido de Icetex: https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/Gestion_documental/PresentacionPoliticaGestionDocumental2014.pdf

Invima. (17 de 03 de 2017). *Instituto Nacional de Vigilancia de Medicamentos y Alimentos*. Obtenido de Invima: https://www.invima.gov.co/images/stories/formatotramite/GDI-DIE-PL020.pdf

MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1 - Método. (Octubre de 2012). Obtenido de http://bit.ly/1QJQOs4

MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 2 - Catalogo. (Octubre de 2012). Obtenido de http://bit.ly/1QJQOs4

Ministerio de Tecnologías de la Información y Comunicaciones. (s.f.). Obtenido de Ministerio de Tecnologías de la Información y Comunicaciones: http://www.mintic.gov.co

Otalora, M. E. (s.f.). *Instituto de Transito de Boyaca*. Obtenido de http://www.itboy.gov.co/new/index.php/normatividad/resoluciones

Ponemon Org. (2016). *Ponemon Cost of Data Breach Study.* Obtenido de Ponemon Org.: http://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf

Sosa, J. (27 de enero de 2012). *pegasus.javeriana.edu.co*. Obtenido de http://pegasus.javeriana.edu.co/~CIS1130SD03/Documentos_files/Analisis_de_Riesgos.pdf

Gartner. (2012). The Nexus of Forces: Social, Mobile, Cloud and Information. Disponible en: https://goo.gl/5VNFtK