PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Elaborado por: Ing. Juan Carlos Puentes G.

Profesional Especializado-Sistemas

Tunja, 25 de enero de 2.019

1. OBJETIVO:

Identificar y ejecutar actividades orientadas a fortalecer el aseguramiento de los servicios de TI y la información que se genera, obtiene y para preservar la confidencialidad, integridad y disponibilidad de la información del Instituto de Tránsito de Boyacá - ITBOY.

1.1. Objetivos Específicos:

1.1.1. Fortalecer el aseguramiento de los servicios de TI y la información suministrada o relacionada con los usuarios de Instituto de Tránsito de Boyacá, mediante la medición de la Implementación del Modelo de Seguridad y Privacidad de la Información.

1.1.2. Fomentar en los procesos de la Entidad, la gestión de riesgos de seguridad de la información, con base en los activos previamente identificados y las acciones para mitigar el riesgo.

1.1.3. Ejecutar actividades en el marco de una metodología de gestión de la seguridad, para establecer un modelo de madurez aplicable y repetible.

1.1.4. Definir y socializar políticas, lineamientos, buenas prácticas y recomendaciones para establecer cultura en Seguridad de la Información en la Entidad.

2. ALCANCE:

A través de este documento se pretende analizar los riesgos y amenazas del proceso de apoyo tecnológico, que contempla los lineamientos establecidos para regular las comunicaciones tanto internas como externas, que apoyan la misión institucional del ITBOY.

El uso y los recursos informáticos que se encuentran al servicio del Instituto de Tránsito de Boyacá, sean o no de propiedad del mismo, sea que estén compartidos o controlados individualmente, aislados o interconectados a redes. Los recursos incluyen los datos, la información electrónica, software, los equipos de cómputo y comunicaciones.

3. DEFINICIONES:

Confidencialidad: Propiedad que impide la divulgación de información a personas o sistemas no autorizados.

Disponibilidad: Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

Integridad: garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento.

Seguridad: Protección de los activos de información, contra amenazas que garanticen la continuidad del negocio, minimizando el riesgo y maximizando las oportunidades de la unidad

4. JUSTIFICACION

El Instituto de Transito de Boyacá requiere la implementación del Plan de Seguridad y privacidad de la Información a fin de dar cumplimiento a la normatividad vigente que obliga el adecuado tratamiento de la información manejada por la Entidad en términos de confidencialidad, integridad y disponibilidad. Entre otras se citan:

- **Ley 1437 de 2011, Capítulo IV**, "*utilización de medios electrónicos en el procedimiento administrativo*". *"Los procedimientos y trámites administrativos podrán realizarse a través de medios electrónicos. Para garantizar la igualdad de acceso a la administración, la autoridad deberá asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros procedimientos.*"

- **Ley 1581 de 2012**, g) Principio de seguridad: *"La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.*"

- **Ley 1581 de 2012, Artículo 17, ítem d**: "*Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento*"

- **Ley 1712 de 2014**, "*principio de transparencia*": "*Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta ley se presume pública, en consecuencia de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta ley.*"

- **Ley 1712 de 2014, artículo 7**: "*Disponibilidad de la información*""*En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o*

locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten."

- **Ley 1712 de 2014** -Título III "*Excepciones acceso a la información*" "*Información exceptuada por daño de derechos a personas naturales o jurídicas. Es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito.*"

- **Decreto 2573 de 2014**:"*Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea…*" donde se encuentra como componente el modelo de Seguridad y Privacidad de la Información.

- **Decreto 1413 de 2017**, artículo 2.2.17.6.6, "*Seguridad de la información.*" "*Los actores que traten información, en el marco del presente título, deberán adoptar medidas apropiadas, efectivas y verificables de seguridad que le permitan demostrar el correcto cumplimiento de las buenas prácticas consignadas en el modelo de seguridad y privacidad de la información emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones, o un sistema de gestión de seguridad de la información certificable. Esto con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información.*"

- **Decreto 1413 de 2007**, artículo 2.2.17.6.1, "*Responsable y encargado del Tratamiento*:"Los operadores de servicios ciudadanos digitales serán responsables del tratamiento de los datos personales que los ciudadanos le suministren directamente y encargados del tratamiento respecto de los datos que otras entidades le proporcionen."

- **Artículo 2.2.17.6.3**, "*Responsabilidad demostrada*"."*Los operadores de servicios ciudadanos digitales deberán adoptar medidas apropiadas, efectivas y verificables que le permitan demostrar el correcto cumplimiento de las normas sobre tratamiento de datos personales. Para el efecto, deben crear e implementar un Programa Integral de Gestión de Datos (PIGD), como mecanismo operativo para garantizar el debido tratamiento de los datos personales.*"

- **Decreto 1413 de 2007**, artículo 2.2.17.6.5, "*Privacidad por diseño y por defecto*":*"Los operadores de servicios ciudadanos digitales deberán atender las buenas prácticas y principios desarrollados en el ámbito internacional en relación con la protección y tratamiento de datos personales que son adicionales a la Accountability, y que se refieren al Privacy by design (PbD) y Privacy Impact Assessment (PIA), cuyo objetivo se dirige a que la protección*

de la privacidad y de los datos no puede ser asegurada únicamente a través del cumplimiento de la normativa, sino que debe ser un 'modo de operar de las organizaciones, y aplicarlo a los sistemas de información, modelos, prácticas de negocio, diseño físico, infraestructura e interoperabilidad, que permita garantizar la privacidad al ciudadano y a las empresas en relación con la recolección, uso, almacenamiento, divulgación y disposición de los mensajes de datos para los servicios ciudadanos digitales gestionados por el operador"

- **Decreto 1413 de 2017**, artículo 2.2.17.5.10, "*Derechos de los usuarios de los servicios ciudadanos digitales*":

1. *Registrarse de manera gratuita eligiendo al operador de servicios ciudadanos digitales de su preferencia entre aquellos que estén vinculados por el articulador.*
2. *Aceptar, actualizar y revocarlas autorizaciones para recibir información, comunicaciones y notificaciones electrónicas desde las entidades públicas a su elección a través de los servicios ciudadanos digitales.*
3. *Hacer uso responsable de los servicios ciudadanos digitales a los cuáles se registre.*
4. *Interponer peticiones, quejas, reclamos y solicitudes de información en relación con la prestación a los servicios ciudadanos digitales.*
5. *Elegir y cambiar libremente el operador de servicios ciudadanos digitales*
6. *Solicitar en cualquier momento, y a través de cualquiera de los medios de atención al usuario, su retiro de la plataforma de servicios en· cuyo caso podrá descargar su información a un medio de almacenamiento propio.*

- **Decreto 1413 de 2017**, artículo 2.2.17.2.1.1 "*Descripción de los servicios ciudadanos digitales, 1.5 servicio de interoperabilidad: Cualquier desarrollo en el marco de los servicios ciudadanos digitales especiales deberá hacer uso de o estar soportado en los servicios ciudadanos digitales básicos cuando lo requieran."*

- **Decreto 612 de 2018, artículo** 1. *"Integración de planes institucionales y estratégico. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web."*

- **Conpes 3854 de 2016,** objetivo general *"Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo*

anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país".

Por lo anterior, el Instituto de Transito de Boyacá debe emprender acciones orientadas a la protección de la información que gestiona, realizando la identificación y tratamiento de riesgos de la información de los activos críticos que la soportan, de manera que se establecen y realiza el seguimiento a dichas acciones en el marco del plan de acción y del Sistema Integrado de Gestión.

5. ANTECEDENTES

5.2. Políticas de seguridad de información

Por medio del Manual "Políticas de Seguridad Informática" MN-GET-01, en su versión 4 de fecha 30 de enero 2019 firmada y aprobado, se adoptan las políticas de Seguridad de la Información aplicables a funcionarios, usuarios y terceros que accedan a la información del Instituto, se pretende proteger la información de amenazas, garantizando la continuidad, así como minimizar los posibles daños y maximizar el rendimiento de las inversiones y las oportunidades de negocio. Es importante subrayar que la seguridad de la información no es sinónimo de seguridad informática. La seguridad de la información efectivamente incluye aspectos técnicos, pero se extiende también al ámbito de la organización y contempla aspectos que son estrictamente jurídicos.

5.3. Levantamiento de inventarios de activos de información

En el año 2018, en el marco del Sistema Integrado de Gestión y el Subsistema de Gestión de Seguridad de la Información, los 12 procesos de la Entidad realizaron el levantamiento de los activos de información con base en el procedimiento de "Análisis de activos de información". Este insumo permitió, dar cumplimiento a lo establecido en la Ley 1712 de 2014.

5.4. Elaboración de matriz de riesgos

Teniendo en cuenta las actividades ejecutadas en periodos anteriores, el proceso de Gestión Tecnológica generó la matriz de riesgos de seguridad de la información, con un total de 20 riesgos Identificados, conforme a la Metodología de Administración Gestión de Riesgos de la Entidad, lo que permitirá durante la vigencia 2019 gestionar los riesgos identificados por proceso.

5.5. Plan de tratamiento de riesgos

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.

Para la vigencia 2019 el ITBOY implementara los controles requeridos para el tratamiento de los riesgos identificados en busca de cumplir con los estándares establecidos en la norma ISO/IEC 27002:2005, como guía de buenas prácticas, lo cual permitirá mitigar los riesgos, amenazas y vulnerabilidades del proceso de Gestión Tecnológica existentes en el ITBOY.

5.6. Plan de socialización

El proceso de Gestión Tecnológica realizara durante la vigencia 2019 un plan de sensibilización, mediante el cual se generaron boletines informativos enviados masivamente y de forma articulada con el proceso de Comunicaciones.

5.7. Modelo de Seguridad y privacidad de la información

El proceso de Gestión Tecnológica durante el segundo semestre de la vigencia 2019 realizará mediciones de la evaluación de la implementación del Modelo de Seguridad y Privacidad de la Información de acuerdo a la metodología establecida por el MinTIC – MSPI.

6. ACTIVIDADES VIGENCIA 2019:

El proceso de Gestión Tecnológica proyecta las actividades en el marco del Plan de Acción – Modelo Integrado de planeación y Gestión, teniendo en cuenta los procedimientos documentados e implementados en el Instituto de Transito de Boyacá:

PD-GET-01 ADMINISTRACION DE SERVICIOS ANTIVIRUS
PD-GET-02 ADMINISTRACION RECURSOS ALMACENAMIENTO
PD-GET-03 ADMINISTRACION USUARIOS Y RED
PD-GET-04 COPIAS DE SEGURIDAD
PD-GET-05 MANTENIMIENTO PREVENTIVO Y CORRECTIVO
PD-GET-06 ADMINISTRACION DEL CANAL DE COMUNICACIONES INTERNET
PD-GET-07 ADMINISTRACION DE CLAVES DE ACCESO
PD-GET-08 MODIFICACION DE REGISTRO A TRAVES DE ACCESOS REMOTOS
PD-GET-09 PRUEBAS ADECUACIONES A LOS SISTEMAS DE INFORMACION
PD-GET-10 ADMINISTRACION DE LA PAGINA WEB INSTITUCIONAL

A continuación se relacionan las actividades a realizar de forma articulada con el plan de acción Institucional.

6.1. Socializar boletines informativos o recomendaciones de seguridad:

Para que la información sobre Seguridad de la Información llegue a todos los procesos de la Entidad, se hace necesario contar con la ayuda de los demás proceso del SIG, los cuales deben replicar los tips, noticias, boletines y buenas

prácticas de seguridad de la información.

6.2. Proveedores Críticos:

El objetivo de la actividad de identificación de proveedores críticos es tener el inventario de los terceros que proporcionan o soportan servicios necesarios para la operación del Instituto de Transito de Boyacá, para la identificación del inventario se requiere que todos los procesos se involucren en esta actividad.

6.3. Riesgos de activos críticos:

Los riesgos de seguridad de información son asociados a los activos críticos de información definidos y categorizados por cada proceso de la Entidad, con base en la metodología de generación de inventario de activos de información establecido en el marco del Sistema Integrado de Gestión, conforme a la Metodología de Administración Gestión de Riesgos del Instituto de Transito de Boyacá.

6.4. Respaldo de información:

Para proteger la información almacenada en los equipos de cómputo, los usuarios deberán realizar el respaldo de la información, en los servicios dispuestos por el proceso de Gestión Tecnológica.

6.5. Control de direcciones IP:

Todo equipo de Cómputo que se conecte a la red del Instituto de tránsito de Boyacá, debe incluirse dentro del rango de direcciones de IP fijas establecidas por la oficina de sistemas quién controlará y habilitara el direccionamiento requerido de acuerdo a las normas establecidas por la Organización de Internacional de telecomunicaciones, según las cuales se ajustan al principio de direccionamiento Privado Clase C para IPV4.

7. Cronograma Plan de Seguridad y Gestión de la Información.

No.	Actividad	Responsable	Cobertura	Fecha Inicio	Fecha Final
1	Socializar boletines informativos o recomendaciones de seguridad	Procesos Gestión Tecnológica y Comunicaciones	100% Procesos Institucionales	04/03/2019	31/12/2019
2	Identification de Proveedores Críticos	Procesos Institucionales	100% Procesos Institucionales	04/03/2019	31/12/2019

3	Identificación Riesgos de activos críticos	Procesos Gestión Tecnológica	100% Procesos Institucionales	01/04/2019	31/12/2019
4	Realizar Backup de Respaldo de la información	Procesos Institucionales	100% Procesos Institucionales	06/05/2019	17/05/2019
5	Realizar Control de direcciones IP	Procesos Gestión Tecnológica	100% Procesos Institucionales	18/02/2019	22/02/2019