## 1. CAMBIOS EFECTUADOS

| Versión | Descripción del Cambio | Fecha Aprobación |
|---|---|---|
| 0 | Procedimiento emitido en Versión 0 para prueba. | 22-12-2011 |
| 1 | Actualización de las políticas, cambio de logo institucional | 26-08-2014 |
| 2 | Actualización de las políticas | 17/11/2016 |
| 3 | Actualización de las políticas | 30/07/2018 |
| 4 | Actualización de las políticas | 28/01/2019 |
| 5<br>4 | Actualización de las políticas ítem 19.2" **CONTROL DE UTILIZACIÓN DE EQUIPOS DE CÓMPUTO·** | 28-05-2019 |

## INTRODUCCIÓN

La información es el recurso más importante de cualquier compañía, por ser el único que no se puede o es muy difícilmente remplazable. Al mismo tiempo, es el recurso que está sujeto a mayores vulnerabilidades.

La seguridad de la información pretende proteger a la información de amenazas, garantizando la continuidad de cualquier institución, 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

Hoy por hoy no ciertamente puede hablarse de un sistema 100% seguro, así como la tecnología avanza a pasos agigantados garantizando oportunidad en la información, proceso de datos velocidades extraordinarias, posibilidad de realizar transacciones no presenciales y hasta video conferencias que permiten convertir los negocios en verdaderas mesas virtuales de trabajo; igualmente la vulnerabilidad ante la intromisión no autorizada de hackers y virus informáticos entre otros , incremental el riesgo de posibles sabotajes, robos de datos y adulteración de registros.

No hay un lugar en donde los datos o comunicaciones corporativas sean más vulnerables que en la línea frontal de una organización: Servidores, CCTV, computadores de escritorio, sistemas de comunicaciones, celulares y portátiles de los empleados.

En este sentido, las Políticas de Seguridad Informática (PSI), surgen como una herramienta organizacional para concientizar a cada uno de los funcionarios que hacen parte del Instituto sobre la importancia y sensibilidad de la información y servicios críticos.

El éxito de la Seguridad Informática radica en entender que esta no tiene una solución definitiva aquí y ahora, sino que es y será el resultado de la innovación tecnológica, a la par del avance tecnológico, por parte del área de Sistemas del Instituto en apoyo constante de la parte directiva y control interno como los responsables en

busca de lograr la integridad de nuestro sistema.

**Glosario**

- **CCTV**: Es una sigla en inglés "closed circuit televisión" que traducido al español es "circuito cerrado de televisión", consiste en una o más cámaras de vigilancias conectadas a uno o más monitores de video o televisores que reproducen las imágenes transmitidas por las cámaras.

- **Control de Acceso**: Es la habilidad de permitir o denegar el uso de un recurso particular a una entidad en particular.

**Generalidades**

**Vulnerabilidad informática.** Ausencia o deficiencia que permite violar las medidas de seguridad informáticas para poder acceder a un canal de distribución o a un sistema específico de forma no autorizada y emplearlo en beneficio propio o como origen u objetivo de ataques por parte de terceros.

**Seguridad Física y del Entorno:** Tener implantados controles de acceso físico y mecanismos de identificación y autenticación que protejan contra acceso físico no autorizado a las áreas que almacenan los recurso de información o informáticos usados para la prestación de los servicios y dichos controles son monitoreados de forma continua, manteniendo el registro de los accesos y resguardando los registros de CCTV generados por acceso a los centros de datos.

**BIOMÉTRICO:** Sistema de Información de control de acceso de Funcionarios que permite registrar los ingresos y salidas de los funcionarios mediante un control de identificación por huella digital (biometría)

**AREA SEGURA:** Espacio físico donde se almacena o procesa información crítica de la entidad.

Se consideran áreas seguras:

1. Centro de cómputo, de comunicaciones, cuarto de equipos.
2. Cuartos de centro de cableado
3. Áreas de gestión documental, radicación y archivo
4. Cuartos de UPS y banco de baterías
5. Cuarto de monitoreo del Circuito Cerrado de Televisión (CCTV) de vigilancia

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

Las políticas aplican a funcionarios, contratistas y otros usuarios quienes contando con la debida autorización necesitan utilizar los recursos informáticos que se encuentran al servicio del Instituto como una herramienta para el

cumplimiento de sus deberes o su gestión en favor de la misión del ITBOY

**Responsabilidad:** Es responsabilidad de cada usuario utilizar los recursos informáticos en forma apropiada, de la manera detallada descrita, en beneficio de los intereses del Instituto.

La palabra responsabilidad proviene del latín RESPONDERE, que se refiere a la capacidad de una persona para responder de los hechos propios. Conforme a la doctrina el término responsabilidad significa la sujeción de una persona que vulnera el deber de conducta impuesto en interés de otro sujeto a la obligación de reparar el daño producido. La responsabilidad además de ser un elemento del concepto de Estado de Derecho también es un principio que surge en nuestra Constitución Política, el artículo 6 nos anuncia: "**Los particulares sólo son responsables ante las autoridades por infringir la Constitución y las leyes. Los servidores públicos lo son por la misma causa y por omisión o extra limitación en el ejercicio de sus funciones**".

Asimismo, el artículo 90 de la Carta preceptúa que: "El Estado responderá patrimonialmente por los daños antijurídicos que le sean imputables causados por la acción o la omisión de las autoridades públicas. En el evento de ser condenado el Estado a la reparación patrimonial de uno de tales daños, que haya sido consecuencia de la conducta dolosa o gravemente culposa de un agente suyo, aquél deberá repetir contra éste".

**Cumplimiento.** Cualquier funcionario u otro usuario que haya violado esta política pueden quedar sujeto a una acción disciplinaria.

**ALCANCE DE LAS POLÍTICAS DE SEGURIDAD** Las políticas definidas el presente documento aplican a todos los funcionarios públicos, contratistas y pasantes del Instituto de Tránsito de Boyacá "ITBOY", personal temporal y otras personas relacionadas con terceras partes que utilicen recursos informáticos.

## 1. OBJETIVO

La dirección del **INSTITUTO DE TRANSITO DE BOYACA**, 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, todo 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 estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de ITBOY:
- Garantizar la continuidad del negocio frente a incidentes.

- Determinar los roles y responsabilidades a los funcionarios asignados para el equipo responsable de seguridad de la información de ITBOY.
- **ITBOY** ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

## 2. ALCANCE

Esta política aplica a funcionarios, contratistas y otras partes interesadas, en todos los niveles de **ITBOY,** como parte de su práctica y gestión en los procesos estratégicos, misionales, de apoyo y evaluación

## 3. RESPONSABILIDAD

Es responsabilidad de cada usuario utilizar los recursos informáticos en forma apropiada, de la manera detallada descrita, en beneficio de los intereses del Instituto.

Además de lo contemplado en el Código único Disciplinario capitulo segundo “DEBERES” Artículo 34 especialmente en los literales 21 “Vigilar y salvaguardar los bienes y valores que le han sido encomendados y cuidar que sean utilizados debida y racionalmente de conformidad con los fines a que han sido destinados” y 22 ”Responder por la conservación de los útiles, equipos y muebles confiados a su guarda y administración y rendir cuentas oportunas de su utilización”

## 4. CUMPLIMIENTO

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política. Cualquier funcionario u otro usuario que haya violado esta política pueden quedar sujeto a una acción disciplinaria.

## 5. DEFINICIONES Y VOCABULARIOS

**Política:** Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

**Estándar:** Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

**Mejor Práctica:** Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

**Guía:** Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al

implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

**Procedimiento:** Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca cómo les sea posible, y a la vez se ajustaran a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

**Activo.** Es un objeto o recurso de valor empleado en una empresa u organización

**AUP:** Política de Uso Aceptable

**Amenaza.** Es un evento que puede causar un incidente de seguridad en una empresa u organización produciendo pérdidas o daños potenciales en sus activos.

**Análisis.** Examinar o descomponer un todo detallando cada uno de los elementos que lo forman a fin de terminar la relación entre sus principios y elementos.

**Control.** Es un mecanismo de seguridad de prevención y corrección empleado para disminuir las vulnerabilidades

**Firewall:** Sistema o grupo de ellos enfocados hacia una política de control de acceso entre la red de la organización y redes externas (por ej: Internet).

**Host:** En líneas generales, servidor o estación de trabajo conectado a la red

**LAN:** Local Área Network o Red de Área Local.

**Proxy:** Servicio de propósito especial, código de aplicación instalado en un firewall.

**Proxy server**: permite que el administrador de la red permita o rechace determinados servicios de una aplicación en particular.

**PPP:** Point to Point Protocol. Protocolo comúnmente utilizado para conexiones por modem.

**Red:** Conjunto de máquinas interconectadas entre sí que comparten recursos.

**RFC:** Request for Comment. Se utiliza para establecer y documentar estándares en Internet.

| | ELABORÓ: | REVISÓ | APROBÓ: |
|---|---|---|---|
| NOMBRE | JUAN CARLOS PUENTES GORDO | CESAR JULIAN PEDREROS RUA | WILLIAM DANIEL SILVA SOLANO |
| CARGO | PROF. ESPECIALIZADO SISTEMAS | ASESOR PLANEACIÓN Y SISTEMAS | GERENTE GENERAL |
| FECHA | 22-05-2019 | 24-05-2019 | 28-05-2019 |

**Riesgo.** Es la probabilidad de ocurrencia de un evento que puede ocasionar un daño potencial a servicios, recursos o sistemas de una empresa.

**SLIP:** Serial Line Interface Protocol. Protocolo comúnmente utilizado para conexiones por modem.

**TCP/IP: TCP o "Transfer Control Protocol" / IP: "Internet Protcol",** conjunto de Protocolos utilizados en Internet.

**Vulnerabilidad.** Es una debilidad que puede ser explotada con la materialización de una o varias amenazas a un activo.

## 6. PRINCIPIOS DEL SGSI ITBOY

A continuación se establecen 12 principios de seguridad que soportan el SGSI de ITBOY:

- Las responsabilidades frente a la seguridad de la información se definirán, compartirán, publicaran para que se han aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
- ITBOY: protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- ITBOY: protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- ITBOY: protegerá su información de las amenazas originadas por parte del personal.
- ITBOY: protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- ITBOY: controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- ITBOY: implementará control de acceso a la información, sistemas y recursos de red.
- ITBOY: garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- ITBOY: garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- ITBOY: garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

- ITBOY: garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

## 7. POLITICAS DE SEGURIDAD SGSI ITBOY

A continuación se establecen las 13 políticas de seguridad que soportan el **SGSI** de **ITBOY**:

- ITBOY: ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

- ITBOY: Se compromete a definir, informar, compartir y publicar las políticas de seguridad de la información para que estas se han aceptadas por cada uno de los empleados, contratistas o terceros.

- ITBOY: Proteger la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.

- ITBOY: Proteger la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- ITBOY: Proteger su información de las amenazas originadas por parte del personal.

- ITBOY: Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- ITBOY: Controlar la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- ITBOY: Implementará control de acceso a la información, sistemas y recursos de red.

- ITBOY: Establecer que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- ITBOY: Permitir a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- ITBOY: Permitir la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

| | ELABORÓ: | REVISÓ | APROBÓ: |
|---|---|---|---|
| **NOMBRE** | JUAN CARLOS PUENTES GORDO | CESAR JULIAN PEDREROS RUA | WILLIAM DANIEL SILVA SOLANO |
| **CARGO** | PROF. ESPECIALIZADO SISTEMAS | ASESOR PLANEACIÓN Y SISTEMAS | GERENTE GENERAL |
| **FECHA** | 22-05-2019 | 24-05-2019 | 28-05-2019 |

- ITBOY: Garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.
- ITBOY: Garantizar la asignación de roles y responsabilidades dentro de ITBOY que permita el cumplimiento de las funciones asignadas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

## 8. POLITICA DE SEGURIDAD EN REDES

Se debe velar por contar con mecanismos que protejan los recursos informáticos valorados tanto por la inversión económica que representa cada dispositivo físico si no salvaguardar la información que representa el mayor activo de cualquier institución.

El área de sistemas del ITBOY, será la encargada de crear usuarios y asignación de claves de acceso a los sistemas de información que calificándose como de máximo riesgo y de carácter confidencial deberán reposar bajo custodia en caja fuerte del Instituto a los cuales únicamente tendrá acceso y será de absoluta responsabilidad el Profesional especializado de Sistemas y la Gerencia General, está solo en caso extremo. De ser abierto este sobre deberá procederse de inmediato a realizar el cambio de todos los Password y usuarios.

## 9. PRIVACIDAD EN LA RED Y CONTROL DE INTRUSOS (PRIV)

### 9.1 Privacidad en la Red

Las comunicaciones son la base de operación que garantiza la oportunidad

Ofreciendo así l a prestación eficiente de los servicios y manejo de negocios en el mundo moderno del cual hacernos parte. Por tal razón, es necesario implementar medidas que alejen de los servidores, datos e instalaciones hackers y piratas.

El mantener una red segura fortalece la confianza de nuestros usuarios frente a nuestra Institución y mejora nuestra imagen corporativa, ya que son innumerables los criminales informáticos (agrupaciones, profesionales, aficionados y accidentales) que asedian día a día las redes. De forma cotidiana estos hackers aportan novedosas técnicas de intrusión, códigos malignos más complejos y descubren nuevos vacíos en las herramientas de software.

### 9.2 Definición de Privacidad de las Redes

Las redes son sistemas de almacenamiento, procesamiento y transmisión de datos que están compuestos de elementos de transmisión (cables, enlaces inalámbricos, satélites, routers switches, entre otros , etc.)

Conectadas a las redes existe un número cada vez mayor de aplicaciones (sistemas de entrega de correo electrónico, navegadores, etc.) y equipos terminales (servidores, teléfonos Ip, computadores de escritorio, portátiles, teléfonos celulares, etc.).

Las redes en el Instituto, son los medios que permiten la comunicación de los equipos de Cómputo y usuarios, pero lamentablemente también están propensasa ser controladas o accesadas por personas no autorizadas. Cuando se refiere a la privacidad de la red, se evoca al cuidado o medidas establecidas para que la información de los sistemas como puede ser datos de nuestros usuarios, reportes financieros y administrativos, estrategias de mercado, etc., no sea consultada por intrusos.

**9.3 Requisitos para Mantener la Privacidad de las Redes**

**9.3.1 Disponibilidad:** significa que los datos son accesibles, inclusive en casos de alteraciones, cortes de energía eléctrica, accidentes o ataques. Esta característica es particularmente importante cuando una avería de la red puede provocar interrupciones o reacciones en cadena que afecten las operaciones

**9.3.2 Autenticación:** Confirmación de la identidad de usuarios. Son necesarios métodos de autenticación adecuados para el acceso a las aplicaciones como El Sistema Integrado de Información de Tránsito de Boyacá SIITBOY, el acceso a los sitios web con los que cuenta el Instituto como Configuración y actualización del Sistema de Gestión de Contenidos Joomla sobre el cual se administra la Página del Itboy, el Próxy, los servidores etc.

**9.3.3 Integridad:** confirmación de que los datos que han sido enviados, recibidos o almacenados son completos y no han sido modificados. La integridad es especialmente importante en relación con la en los casos en los que la exactitud de los datos es crítica como migración de registros a la concesión RUNT, y datos contables entre otros.

**9.3.4 Confidencialidad:** protección de las comunicaciones o los datos almacenados contra su interceptación y lectura por parte de personas no autorizadas. La confidencialidad es necesaria para la transmisión de datos sensibles.

**9.3 Riesgos o Amenazas a la Privacidad de las Redes**

**9.3.1 Acceso no Autorizado a Computadores y Redes:** el acceso no autorizado a computadores o redes de computadores se realiza normalmente de forma mal intencionada para copiar, modificar o destruir datos, aprovechando la tendencia de la mayoría de usuarios a utilizar contraseñas previsibles o la tendencia revelar información a personas en apariencia confiables, es por tanto necesario campañas de concientización y valoración de información, el Instituto debe insistir en la necesidad de fomentar charlas desde el área de sistemas o personal con experiencia que sensibilice al personal y lo

apersone de un proceso tan importante, al que generalmente no se le da la importancia frente al tema de compartir usuarios y contraseñas que pudieran provocar infiltración a las bases de datos del Instituto.

**9.3.2 Ejecución de Programas que Modifican y Destruyen los Datos:** los computadores funcionan con programas informáticos, pero lamentablemente, los programas pueden usarse también para desactivar, borrar o modificar datos. Cuando esto ocurre en un computador que forma parte de una red, los efectos de estas

Alteraciones pueden tener un alcance considerable. Un ejemplo claro son los virus (programa informático mal intencionado que reproduce su propio código y se adhiere, de modo que cuando se ejecuta el programa informático infectado se activa el código del virus y es posible incluso su reproducción).

**4.3.3 Detección de Intrusos**

Los sistemas y aplicaciones están en permanente evolución en busca de la modernidad tecnológica, situación noble y admirable sin embargo a la par con esta evolución surgen nuevos puntos vulnerables. A pesar de los avances en los sistemas de seguridad, los usuarios no autorizados con herramientas muy sofisticadas tienen grandes posibilidades de acceder a las redes, sistemas o sitios de las entidades con el ánimo de malograr sus operaciones.

Actualmente, existen innumerables sitios en internet orientados a la piratería o intrusión de redes, los cuales ofrecen programas de fácil descarga y acceso que han dejados las puertas abiertas para nuevos ataques.

- Los sistemas operativos difícilmente algún día estarán protegidos en su totalidad, incluso si se protege el sistema nuevas vulnerabilidades aparecerán en el entorno todos los días, como las que actualmente representan los teléfonos celulares, equipos inalámbricos y dispositivos de red.

- Actualmente el direccionamiento público enrutado hacia las redes internas permiten que funcionarios se conectan a la red desde la casa, otras oficinas u hoteles fuera del Instituto, lo cual genera nuevos riesgos.

- Falta de malicia por parte de la mayoría empleados que se ausentan y dejan desprotegido su computador.

- Los Funcionarios deben reconocer la importancia de las políticas de seguridad: La capacitación y recomendaciones que se les brinde no cuentan mucho si se ignoran las advertencias sobre los peligros de abrir archivos adjuntos sospechosos del correo electrónico.

**9.3.4 Medidas para Controlar el Acceso de Intrusos**

- El Instituto cuenta además del firewall con un sistema para la administración de la red a través de dos Proxy-Cache para la gestión de los servicios de internet que además permite el monitoreo de

conexión (MRTG), reporte de navegación (SARG),control ancho de banda (HTB),generación de listas negras de navegación con el objeto de bloquear el tráfico no deseado de la red, bloqueador de programas P2P administrador mediante una interfaz gráfica

(WEBMIN) sobre una plataforma en sistema operativo Linux Fedora Core que ofrece mayor robustez e invulnerabilidad frente a posibles contagios informáticos.

- El Instituto realiza la renovación anual de las licencia del antivirus del tipo corporativo ( Kaspersky) encaminada hacia la detección y remoción de virus, malware, Sistemas realiza periódicos procesos de mantenimiento incluyendo limpieza de cache de servidores

- Constantemente se monitorea y depuran los servicios a fin de desactivar los servicios innecesarios de las redes.

- Constantemente se crean respaldos o backups de los datos de los servidores.

- 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.

- A todos los equipos de cómputo del Instituto de Tránsito de Boyacá, el área de sistemas deberá identificar plenamente las características propias y el funcionamiento responsable de los mismos.

- Los Servidores del Instituto de Tránsito de Boyacá, requieren de ubicación aislada en un cuarto de comunicaciones provisto de un Rack, Switche KVM para administración, en condiciones ambientales y adecuadas, el acceso a este cuarto estará restringido solo a personal autorizado.

- A protección física de los equipos corresponde a quien en principio se le asigne y corresponde informar de los movimientos en caso de que existan a la oficina de sistemas, quien deberá realizar las respectivas actualizaciones en las respectivas hojas de vida de la máquina y generar los permisos correspondientes.

- En cuanto a los equipos de terceros, el área de sistemas determinará su necesidad y autorizará su ingreso al Instituto así como evaluará y aprobará la utilización de los mismos, estableciendo pautas que eviten una violación a los sistemas de Información y canales de comunicación.

- El uso de Dispositivos externos de almacenamiento se encuentra restringido y ninguno sin autorización de sistemas puede ser utilizado para extraer o incorporar información a los equipos del ITBOY, para esto el sistema impide la instalación de los mismos.

## 10. VIRUS Y ANTIVIRUS V/A

Los virus informáticos son básicamente programas, y como tales hechos por programadores. Que debido a sus características particulares son especiales. Para hacer un virus de computadora no se requiere capacitación especial, ni una genialidad significativa, sino conocimientos de lenguajes de programación y algunos conocimientos puntuales sobre el ambiente de programación y arquitectura de las PC's.

Desde sistemas se detecta el problema del virus, desde el punto de vista funcional.
En la vida diaria, cuando un programa invade inadvertidamente el sistema, se replica sin conocimiento del usuario y produce daños, pérdida de información o fallas del sistema, reconocemos que existe un virus. Los virus actúan enmarcados por "debajo" del sistema operativo, como regla general, y para actuar sobre los periféricos del sistema, tales como disco Duro, Memorias Usb, ZIP's CD-R's, hacen uso de sus propias rutinas aunque no exclusivamente. Un programa normal, por llamarlo así, utiliza las rutinas del sistema operativo para acceder al control de los periféricos del sistema, y eso hace que el usuario sepa exactamente las operaciones que realiza, teniendo control sobre ellas. Los virus, por el contrario, para ocultarse a los ojos del usuario, tienen sus propias rutinas para conectarse con los periféricos del computador lo que les garantiza cierto grado de inmunidad a los ojos del usuario, que no advierte su presencia, ya que el sistema operativo no refleja su actividad en la PC. Una de las principales bases del poder destructivo de estos programas radica en el uso de funciones de manera "sigilosa", oculta a los ojos del usuario común.

El virus, por tratarse de un programa, para su activación debe ser ejecutado y funcionar dentro del sistema al menos una vez. Demás está decir, que los virus no surgen de las computadoras espontáneamente, sino que ingresan al sistema inadvertidamente para el usuario, y al ser ejecutados, se activan y actúan con la computadora huésped.

### 10.1 Características

Hay que recordar que un virus no puede ejecutarse por sí solo, pues necesita un programa portador para poder cargarse en memoria e infectar; asimismo, para poder unirse en un programa portador, el virus precisa modificar la estructura de aquél, posibilitando que durante su ejecución pueda realizar una llamada al código del virus.

Las particularidades de los virus:

- Son muy pequeños.
- Casi nunca incluyen el nombre del autor, ni el registro o copyright, ni la fecha de creación.
- Toman el control o modifican otros programas.
- Es dañino: El daño es implícito, busca destruir o alterar, como el consumo de memoria principal y tiempo de procesador.
- Es autor reproductor: A nuestro parecer la característica más importante de este tipo de programas es la de crear copias de sí mismo.

- Es subrepticio: Esto significa que utilizará varias técnicas para evitar que el usuario se dé cuenta de su presencia.

**5.2 Síntomas Más Comunes de Virus**

- Los programas comienzan a ocupar más espacio de lo habitual. Se reduce el espacio libre en la memoria RAM. El virus al entrar en el sistema, se sitúa en la memoria RAM, ocupando una porción de ella. El tamaño útil y operativo de la memoria se reduce en la misma cuantía que tiene el código del virus. Siempre en el análisis de una posible infección es muy valioso contar con parámetros de comparación antes y después de la posible infección. Por razones prácticas casi nadie analiza detalladamente su PC en condiciones normales y por ello casi nunca se cuentan con patrones antes de una infección, pero sí es posible analizar estos patrones al arrancar una PC en la posible infección y analizar la memoria arrancando el sistema desde un disco libre de infección.

- Aparecen o desaparecen archivos. En mayor o menor medida, todos los virus, al igual que programas residentes comunes, tienen una tendencia a "colisionar" con otras aplicaciones, lo que provoca también aparición de mensajes de error no comunes.

- Cambia el tamaño de un programa o un objeto. Programas que normalmente funcionaban bien, comienzan a fallar y generar errores durante la sesión.

- Aparecen mensajes u objetos extraños en la pantalla. El código viral, ocupa parte de la RAM y debe quedar "colgado" de la memoria para activarse cuando sea necesario. Esa porción de código que queda en RAM, se llama residente y con algún utilitario que analice el RAM puede ser descubierto.
- El disco trabaja más de lo necesario. Tiempos de cargas mayores y es debido al enlentecimiento global del sistema, en el cual todas las operaciones se demoran más de lo habitual.

- Los objetos que se encuentran en la pantalla aparecen ligeramente distorsionados. Las operaciones se realizan con más lentitud, ya que los virus son programas y como tales requieren de recursos del sistema para funcionar y su ejecución al ser repetitiva, lleva a un enlentecimiento y distorsión global en las operaciones.

- Se modifican sin razón aparente el nombre de los ficheros.

- No se puede acceder al disco duro.

**10.3 Antivirus**

Es el programa que se encarga de analizar el contenido de los ficheros y, en caso de detectar un virus en su interior, proceder a su desinfección. También realizan búsquedas heurísticas, esto es, buscar funciones que puedan resultar nocivas para el computador, sin que sean virus reconocidos.

Es una aplicación o programa dedicada a detectar y eliminar virus informáticos. La forma en que protege es la siguiente, el sistema de protección del Antivirus depende del sistema operativo en que se esté trabajando. En DOS se utiliza TSR (Terminate and Stay Resident, programas que terminan y se quedan

Residentes en memoria), en Windows 95/98 VxD (Virtual Driver) y en NT drivers en modo Kernel. Por término general se puede pensar en un programa que vigila todos y cada uno de los accesos que se realizan a ficheros y discos y antes de autorizarlos avisa de la existencia virus y, en su caso, desinfecta el fichero en cuestión.

**10.4 Controles**

- Control de acceso físico a los equipos.
- Control de entradas a los programas de los computadores a través de claves de acceso (passwords).

## 11. INSPECCION DEL USO DEL SISTEMA

- El administrador del sistema debe realizar periódicamente la inspección. Si no, puede usarse software elaborado con este fin. La inspección de un sistema implica revisar varias de sus partes y buscar cualquier cosa que sea inusual. En esta sección se explican algunas de las formas para hacer esto.
- La inspección debe hacerse con regularidad. No es suficiente hacerla cada mes o cada semana, ya que esto provocaría una brecha de seguridad que no sería detectada en mucho tiempo.
- Algunas violaciones de seguridad pueden detectarse unas cuantas horas después de haberse cometido, en cuyo caso no tiene sentido la inspección semanal o mensual. El objetivo de la inspección es detectar la brecha de seguridad en forma oportuna, de modo que se pueda reaccionar adecuadamente a ella.

## 12. MECANISMOS DE INSPECCION

Muchos sistemas operativos almacenan la información de conexiones en archivos de registro especiales. El administrador del sistema debe examinar regularmente estos archivos de registro para detectar el uso no autorizado del sistema. La siguiente es una lista de métodos que puede utilizar en su sitio.

Puede comparar las listas de los usuarios que estén conectados en ese momento con los registros de las conexiones anteriores. La mayoría de los usuarios tienen horarios de trabajo regulares y se conectan y desconectan casi a la misma hora todos los días.

Una cuenta que muestre actividad fuera del horario “normal” del usuario debe inspeccionarse de cerca. Quizá un intruso este usando esa cuenta. También puede alertarse a los usuarios para que observen el último mensaje de conexión que aparece al momento de hacer su primera conexión. Si notan algún horario inusual, deben avisarle al administrador del sistema.

## 13. HORARIO DE INSPECCION

Los administradores del sistema deben inspeccionar con frecuencia y regularidad a lo largo de todo el día.

## 14. PROCEDIMIENTOS DE ADMINISTRACION DE CUENTAS

Cuando se crean cuentas de usuario, debe tenerse cuidado en no dejar ninguna laguna de seguridad. Si el sistema operativo se está instalando desde los medios de distribución, debe examinarse que la contraseña no tenga cuentas privilegiadas que no se necesite.

Algunos vendedores de sistemas operativos proporcionan cuentas para los ingenieros de servicio de campo y servicios de sistemas. Estas cuentas o no tienen contraseña o son de dominio público. Si se necesita estas cuentas, debe darse una contraseña nueva; si no, debe eliminarse o desactivarse. En general no hay ninguna razón para permitir cuentas que no tienen una contraseña establecida.

Las cuentas sin contraseña son peligrosas aun cuando no ejecuten intérpretes de comandos, como la cuenta que existe tan solo para ver quién está conectado en el sistema. Si estas no están establecidas correctamente, puede comprometerse la seguridad del sistema. Por ejemplo, si no se establece adecuadamente el usuario anónimo de una cuenta FTP a cualquier usuario le estar permitido el acceso al sistema para recuperar archivos. Si se cometen errores al establecer esta cuenta, e inadvertidamente se concede el permiso de escritura al sistema de archivos, un intruso puede cambiar el archivo de contraseñas o destruir el sistema.

Asimismo, cuando un usuario privilegiado abandone la organización, se debe avisar para que se cambie la contraseña de las cuentas privilegiadas.

Además deben cambiarse las cuentas de usuario de quienes se retiran de a Institución

## 15. POLÍTICA DE USO DEL CORREO ELECTRÓNICO

Es responsabilidad de todos los usuarios del Correo Electrónico (E-Mail), seguir los procedimientos establecidos para asegurar un efectivo y eficiente uso del sistema de correo corporativo.

El uso indiscriminado del correo causa degradación en el desempeño del sistema y peor aún, puede resultar en la indisponibilidad del servicio. El sistema de E-Mail depende de la disponibilidad de espacio en disco en los servidores y de las comunicaciones y su uso no adecuado sobrecarga estos recursos.

Es política del Grupo que el sistema de correo (E-Mail) sea para USO DEL INSTITUTO. Por lo tanto, los usuarios deberán abstenerse de enviar mensajes no oficiales, como por ejemplo, videos de saludos/bromas, cartas de cadenas, avisos económicos, etc… ya que estos incrementan el uso de recursos escasos como el espacio en disco y el ancho de banda de las líneas de comunicaciones y además pueden resultar en la diseminación de virus aparte de consumir tiempo productivo del personal.

Para asegurar el uso eficiente del sistema del correo electrónico, se debe seguir las siguientes recomendaciones:

- Envío de Información Confidencial: En el interés de la seguridad, los empleados del SCC deben abstenerse de enviar correos confidenciales y/o críticos para el negocio, a través de Internet. Todo envío de información confidencial debe hacerse vía Fax, que es la herramienta del Grupo para estos efectos.

- Tratar la Internet como un Dominio Público, donde cualquier dicho o juicio hecho por los empleados, necesariamente refleja la posición del SCC. Por lo tanto, sólo personas autorizadas por el SCC para actuar en su representación (p.e. Asuntos Públicos) pueden responder o comentar en Internet, sobre aquellas materias relacionadas con la empresa.

- Evite Anexar Grandes Archivos: Cuando requiera anexar grandes archivos, hágalo fuera de los horarios de alto tráfico o en casos extremos utilice el fax.

  Enviar un archivo muy grande a través de la red toma considerable tiempo y como consecuencia produce congestión y demoras en la entrega de los demás correos.

  Para minimizar los tamaños use siempre la compresión de archivos utilizando la herramienta que se encuentre disponible, teniendo en cuenta en cuenta que sobre 2 MB los correos son rechazados.

- Evite Enviar Correos a Grandes Grupos de Usuarios: Envíe, copie, replique o re- rutee mensajes sólo a aquellos usuarios relacionados con cada tema. Operar sobre la base “estrictamente necesario-de-conocer”.

- Practique Frecuente Limpieza de su Directorio de Correo: Existe una cuota para su espacio en correo, por lo tanto éstos deben ser borrados o si revisten importancia, guardados en archivos personales residentes en la red. De esta forma evitará interrupciones en su servicio por falta de capacidad en disco.

- No Use la Funcionalidad Replicar o Re-Rutear Para Recipientes de Correo Internacional: Envíe un mensaje nuevo (es decir, no anexe el historial de los mensajes que generan esta respuesta). Tome en cuenta que el costo de los correos internacionales está basado en el tamaño de los mismos.
- Uso de Direcciones Personales: Estas no son actualizadas cuando se producen cambios en las listas oficiales de correo, por lo que es responsabilidad de cada uno su permanente actualización.

- Envío de Mensajes Urgentes: De acuerdo al BCP (Business Communications Procedures) todo mensaje URGENTE debe ir acompañado de un llamado telefónico.

- Escriba sus Mensajes Directamente en el Correo: En la medida de lo posible escriba sus mensajes directamente en el correo. Escribir mensajes en Word y luego anexarlos genera mensajes que ocupan un mayor espacio y hacen más lenta su lectura consumiendo más recursos del sistema.

| | ELABORÓ: | REVISÓ | APROBÓ: |
|---|---|---|---|
| **NOMBRE** | JUAN CARLOS PUENTES GORDO | CESAR JULIAN PEDREROS RUA | WILLIAM DANIEL SILVA SOLANO |
| **CARGO** | PROF. ESPECIALIZADO SISTEMAS | ASESOR PLANEACIÓN Y SISTEMAS | GERENTE GENERAL |
| **FECHA** | 22-05-2019 | 24-05-2019 | 28-05-2019 |

## 16. POLÍTICA DE ADMINISTRACIÓN DE PASSWORDS

Uno de los componentes básicos de la Tecnología de la Información es la confidencialidad, es decir la protección de la información sensible del acceso de personas no autorizadas.

Los computadores personales usados para llevar a cabo los negocios de la compañía, en la mayoría de los casos contienen información sensible la cual debe estar protegida de accesos de terceros o más aún de accesos involuntarios. Los "hackers" no están interesados en los PC's como tal, sino en la valiosa información que ellos contienen en sus medios magnéticos.

En vista de lo anterior, se ha preparado esta política para lograr que su cumplimiento garantice la seguridad de la información residente tanto en nuestros PC's como en otras facilidades IT y debe ser adherida por todos los usuarios. A continuación se resume las principales responsabilidades de cada sector:

### 16.1 Para los Administradores de Seguridad: (Administrador de LAN,)

- Ningún sistema debe desplegar la password al momento de ser ingresada.
- Todos los sistemas deben obligar (donde sea posible) a que el largo de la password tenga un mínimo de 6 caracteres y en aquellos usuarios con privilegios, un largo mínimo de 8.
- El acceso a los sistemas se bloquea después de tres intentos fallidos de ingreso de la password.
- Todos los sistemas deben obligar, donde sea posible, a cambiar la password una vez transcurridos 30 días.
- Los administradores o Soporte a Usuarios, según corresponda, darán de alta o revocarán passwords existentes con passwords genéricas, solo cuando esto haya sido solicitado vía mail por el jefe inmediato del usuario a quién se le revoca la password. Los sistemas obligarán al usuario a cambiarla inmediatamente luego del primer ingreso.
- Todos los sistemas, donde sea posible, mantendrán un registro de las 13 últimas passwords usadas con el objeto de prevenir que los usuarios las re- utilicen.
- Las passwords con privilegios se encuentran en sobres cerrados, no son conocidas por nadie y se encuentran guardadas en áreas restringidas.

### 16.2 Para los Usuarios:

- Mantener la password de encendido del PC activada. Esta se establece al momento de instalar cada PC por el Departamento de Informática del SCC.

- Configurar el protector de pantalla con password y activación después de cinco minutos sin actividad. Cada vez que el PC quede desatendido se debe activar manualmente el protector de pantalla evitando así que personas no autorizadas tengan acceso a la información.

- Seleccionar una password con un largo mínimo de 6 caracteres utilizando letras, números, mayúsculas, minúsculas y caracteres especiales siguiendo las reglas establecidas.

- Seleccione passwords robustas difíciles de predecir.

- Nunca construya su password basado en alguno de los siguientes factores:
  - fechas asociadas con el usuario (p.e. cumpleaños, nacimiento, etc.)
  - Números telefónicos
  - Indicador de cargo
  - series de caracteres numéricos o alfabéticos iguales
  - Evite escribir su password en presencia de terceros y mantenga la confidencialidad

- Cambie su password a la primera sospecha de que alguien la conozca.

- Evite re-utilizar antiguas passwords aunque el sistema se lo permita.

- Cambie la password después de 30 días de uso aún si el sistema no se lo exige.(p.e. la password de encendido del PC).

- En caso de haber perdido la password su jefe inmediato deberá solicitar vía mail a soporte a usuarios revocar la password existente.

## 17. POLÍTICA DE ACCESO A INTERNET

La Internet ha llegado a ser un poderoso medio de comunicación y una importante herramienta de búsqueda de información

El acceso a Internet es otorgado, a través de las facilidades tanto locales como internacionales del INSTITUTO, para ayudar a los empleados a ser más efectivos en su trabajo. Su uso está sujeto al monitoreo, A todos aquellos con acceso, se les insta fuertemente a ejercitar el buen juicio cada vez que utilicen Internet. Las gerencias de líneas tienen la responsabilidad de hacer efectivas las sanciones que correspondan, a todos aquellos que infrinjan cualquiera de las condiciones enumeradas a continuación. Todos Los Funcionarios del Instituto deben adherirse a esta política para asegurar el uso seguro y productivo de la Internet incluyendo los equipos de terceros y contratistas que en su momento estén prestando un servicio de carácter institucional y se encuentren en la red de datos del Insituto

- El acceso a Internet provisto debe ser usado sólo para propósitos del ITBOY

- Está estrictamente prohibido la difusión en Internet de documentos relacionados con la institución, programas, objetos y gráficos sin la debida autorización. Los funcionarios tienen la responsabilidad de proteger toda aquella información comercial y/o propietaria que sea propiedad intelectual de la empresa.

- Toda información extraída a través de Internet, a menos que sea de fuentes confiables confirmadas, debe ser validada antes de ser utilizada para fines del ITBOY.

- Todos los archivos extraídos desde internet deben ser scaneados y limpiados de virus. De acuerdo a la política de Control de Virus, acciones disciplinarias se tomarán contra todos aquellos que fallen en tomar precauciones que conduzcan a difundir virus en las redes.

- Cualquier texto, foto, sonido, video u otro objeto gráfico que pueda ser considerado ofensivo (p.e. material pornográfico) o en alguna forma discriminatorio, no debe ser desplegado, almacenado ni transmitido sobre los equipos de propiedad de la compañía. Como empleados, se espera que nos conduzcamos en una forma decente y profesional.

- Está estrictamente prohibido el acoso a individuos, corporaciones u organizaciones y el acceso a cualquier sistema o computador de un tercero sin el expreso consentimiento del propietario. Al cometer tales actos, se queda expuesto a reclamos de tipo legal como individuo.

- Los usuarios de Internet deben reportar todos los problemas de seguridad a Soporte a Usuarios.

- El área de Sistemas es la dependencia responsable de Parametrizar y administrar los recursos de internet mediante la aplicación de criterios que permitan discriminar entre sitios autorizados y no autorizados mediante listas blancas y negras(restricción a sitios como www.youtobe.com, whats app web, spotify entre otros) de navegación que son controlados desde el Proxy que permite la administración de este recurso.

- El área de sistemas mediante evaluación del requerimiento asigna los anchos de banda necesarios para cada dependencia.

- El área de sistemas monitorea a través del proxy la adecuada utilización del recurso de Internet, mediante informes que reflejan la utilización del canal, paginas visitas, tiempo de navegación, frecuencias, estabilidad del canal entre otros.

- Se prohíbe el uso de accesos o programas para realizar conexiones remotas a fin de tomar dominio de las máquinas excepto las estrictamente necesarias, que deben ser de manera temporal y con autorización expresa del área de sistemas, quien evaluará la situación y realizará acompañamiento en la instalación y desinstalación una vez concluida la labor que lo requiera.

## 18. POLÍTICA DE RESPALDO Y RECUPERO DE DATOS

| | ELABORÓ: | REVISÓ | APROBÓ: |
|---|---|---|---|
| **NOMBRE** | JUAN CARLOS PUENTES GORDO | CESAR JULIAN PEDREROS RUA | WILLIAM DANIEL SILVA SOLANO |
| **CARGO** | PROF. ESPECIALIZADO SISTEMAS | ASESOR PLANEACIÓN Y SISTEMAS | GERENTE GENERAL |
| **FECHA** | 22-05-2019 | 24-05-2019 | 28-05-2019 |

El respaldo/recupero tiene como objetivo asegurar la continuidad de los procesos ante pérdida de los datos operacionales guardados en los dispositivos de almacenamiento.

Todo archivo productivo, tendrá una política de back-ups y restore que deberá ser ejecutada por el Responsable de la dependencia en la cual se maneje información que se considere vital para la operatividad del cargo y los intereses del Instituto y la periodicidad del mismo dependerá del criterio del responsable dependiendo del volumen de información.

Los back-ups serán mantenidos en lugares distintos al de procesamiento, en condiciones seguras.

Los backups de aplicaciones que reposan en los servidores del Instituto y de la cual depende la estructura tecnológica del Itboy serán responsabilidad del área de Sistemas.

**19. POLÍTICA ENCAMINADA A LA REALIZACIÓN DE MANTENIMIENTO DE LOS EQUIPOS DE CÓMPUTO.**

- A la oficina de sistemas del Instituto de Tránsito de Boyacá le corresponde elaborar y ejecutar el Plan de mantenimiento preventivo y/o correctivo de los equipos de cómputo de acuerdo a la programación realizada a comienzos del año, e igualmente atender de manera oportuna las solicitudes de mantenimiento requeridas por las diferentes dependencias del Instituto.
- Los equipos de cómputo de terceros que se encuentren operando en las instalaciones del ITBOY, y que el área de sistemas según estudio de necesidad generada por el técnico responsable determine la realización de mantenimiento correctivo, esta dependencia solicitará autorización a la entidad que los proporcionó y si la empresa que los suministro requiere realizarlos por sus medios, deberá solicitar así mismo los permios de ingreso de personal y bajo supervisión de sistemas se realizará dicho mantenimiento.

- Solo personal de sistemas realizará mantenimientos y ningún funcionario diferente está autorizado para realizar adecuación alguna.

**19.1 Actualización de Equipos**

Todos los equipos de cómputo (computadores, servidores, dispositivos activos de red, dispositivos de impresión, canales de comunicaciones, software) que sean propiedad del ITBOY, se deberán actualizar de manera permanente apuntado a nuevas tecnologías en procura de una mejora continua.

**19.2 Control de Utilización de equipos de cómputo.**

- Todos y cada uno de los equipos son asignados a un funcionario del Itboy, por lo que es de su responsabilidad hacer buen uso de este recurso.

| | ELABORÓ: | REVISÓ | APROBÓ: |
|---|---|---|---|
| **NOMBRE** | JUAN CARLOS PUENTES GORDO | CESAR JULIAN PEDREROS RUA | WILLIAM DANIEL SILVA SOLANO |
| **CARGO** | PROF. ESPECIALIZADO SISTEMAS | ASESOR PLANEACIÓN Y SISTEMAS | GERENTE GENERAL |
| **FECHA** | 22-05-2019 | 24-05-2019 | 28-05-2019 |

- El área de sistemas del ITBOY, tiene la facultad de acceder a cualquier equipo que haga parte de la red tanto en la sede principal como los ubicados en los puntos de atención con el ánimo de realizar monitoreo permanente a fin de garantizar la operatividad de cada una de las máquinas y el desempleo de las mismas.

- Solo el área de sistemas es la dependencia autorizada para el traslado, reubicación, desmonte, incorporación al sistema de información del Instituto, de equipos de cómputo, por ninguna circunstancia ningún funcionario podrá tomar este tipo de decisiones, el incumplimiento podrá acarrear sanciones de carácter disciplinario.

- Todos los equipos de cómputo deberán ser identificados mediante la asignación de una dirección IP clase C.

- Todos los equipos de cómputo contarán con usuario administrador para uso exclusivo del área de sistemas y usuario para la operación del mismo, que será asignado al usuario responsable de la máquina, este perfil cuenta con restricciones como cambios de fecha del sistema, cambio de parámetros de red y descarga de software, para el efecto el área de sistemas contará con herramientas como pgedit.msc, secpol.msc

- Todos los equipos se configuran con mensaje de inicio de Windows con las políticas de uso y advertencias por uso inapropiado, el texto es el siguiente:

***"legalnoticecaption : SISTEMAS ***ATENCION******

***legalnoticetext: Este es un equipo de uso oficial y de propiedad del Instituto de Tránsito de Boyacá "ITBOY". Su ingreso es permitido solo para usuarios autorizados. El uso no autorizado o impropio de este sistema puede causar sanciones disciplinarias, civiles y penales. Accediendo a este equipo el usuario está de acuerdo y acepta términos y condiciones. Si usted no es usuario autorizado o no está de acuerdo con las condiciones listadas termine su uso de inmediato."***

**19.3 Control de entrada al Cuarto de Telecomunicaciones**

Se entiende como cuarto de telecomunicaciones al espacio utilizado exclusivamente para alojar los elementos de terminación del cableado estructurado y los equipos de telecomunicaciones.

El diseño de cuartos de telecomunicaciones debe considerar, además de voz y datos, la incorporación de otros sistemas de información del edificio tales como televisión por cable (CATV), alarmas, seguridad, audio, CCTV y otros sistemas críticos.

| | ELABORÓ: | REVISÓ | APROBÓ: |
|---|---|---|---|
| **NOMBRE** | JUAN CARLOS PUENTES GORDO | CESAR JULIAN PEDREROS RUA | WILLIAM DANIEL SILVA SOLANO |
| **CARGO** | PROF. ESPECIALIZADO SISTEMAS | ASESOR PLANEACIÓN Y SISTEMAS | GERENTE GENERAL |
| **FECHA** | 22-05-2019 | 24-05-2019 | 28-05-2019 |

El acceso al cuarto de telecomunicaciones es restringido dado que en éste, se custodian la granja de servidores donde reposan las bases de datos y todo el sistema de comunicaciones del Instituto, por tanto solo personal autorizado podrá ingresar o salvo autorización de esta área.

Este espacio cuenta con sistema de control de acceso biométrico, de tal manera que solo con identificación a través de la huella dactilar podrán acceder el profesional especializado, el técnico de sistemas y para asegurar la entrada en caso de ausencia forzada de estos dos funcionarios se debe habilitar este permiso el asesor de planeación y al gerente.

**20. Pautas de seguridad en áreas seguras: uso equipos de cómputo y monitoreo**

Las estaciones de trabajo y equipos de computación en áreas seguras deben estar ubicados y protegidos adecuadamente, según la naturaleza de la confidencialidad del proceso y de la información que se maneja. Estos equipos deben tener implementados procedimientos de Seguridad que certifiquen su adecuado uso, y evitar así fugas de información. Los colaboradores deben estar monitoreados mediante CCTV de forma permanente

**20.1 Administración de equipos de CCTV.**

Las grabaciones de video con uso de CCTV deben ser monitoreadas y almacenadas con los mecanismos de seguridad y disponibilidad adecuados para su revisión.

- Las cámaras están ubicadas de tal forma que se mantengan vigiladas y monitoreadas las áreas que impliquen el acceso de personal, visitantes y proveedores.

- Las cámaras de vigilancia tienen como objeto exclusivo proteger los bienes físicos del Instituto, al personal y visitantes, así como colaborar con las autoridades en la prevención de actos criminales.

- Bajo ninguna circunstancia se podrán desconectar, manipular (como cambiar la dirección, interferir la transmisión ubicar objetos que reduzcan el objetivo de la cámara, entre otros) o apagar las cámaras

**"Cuando no ocurre nada, nos quejamos de lo mucho que gastamos en seguridad. Cuando algo sucede, nos lamentamos de no haber invertido más... Más vale dedicar recursos a la seguridad que convertirse en una estadística."**