**Diciembre de 2022**

**POLÍTICAS TIC INVISBU**

## INTRODUCCIÓN

Con el propósito de establecer al interior del Instituto de Vivienda Interés Social y Reforma Urbana del Municipio de Bucaramanga – INVISBU, una cultura que garantice el buen uso de las tecnologías de Información y la Comunicación se definen el documento de políticas y lineamientos que contribuyan a la seguridad de los activos de información y que ayudan al efectivo mejoramiento continuo de los procesos que se apoyan en los elementos tecnológicos.

Todos estos aspectos técnicos se deben formalizar y poner en conocimiento de todos los funcionarios de la entidad; con el fin de que conozcan la importancia de cada elemento tecnológico que les permite el mejor desempeño de las funciones.

Este documento enmarca todos los elementos que interactúan a nivel de las TIC y define las mejores tácticas para su uso; así como cada la responsabilidad de cada área.

El definir en forma adecuada cada uno de estos aspectos, hace que el INVISBU pueda cumplir las normas que regulan las TIC, con sus planes, sus objetivos, su misión y su visión; además una vez se socialice se convierte en una herramienta que permitirá llevar a cabo el mejor control y seguimiento del uso de toda la infraestructura tecnológica.

Este documento será susceptible de cambios y ajustes necesarios; de acuerdo a la evolución y sistematización de los procesos al interior de la organización y de las políticas generales del ministerio de tecnologías de información y de la comunicación de Colombia.

## OBJETIVOS

### Objetivo General

Garantizar la integridad, confidencialidad y disponibilidad de las TIC que se utilizan en el INVISBU y que permiten el cumplimiento de las estrategias planteadas en el la política de gobierno Digital, así como el logro de los objetivos del plan estratégico de sistemas “PETI”, el cumplimiento de la normatividad vigente sobre TIC y la satisfacción de sus usuarios.

### Objetivos Específicos

- Elaborar una guía documental que permita identificar las políticas y lineamientos a seguir para el buen uso y cuidado de cada elemento dentro de la infraestructura tecnológica de la Entidad.

- Definir las políticas y lineamientos claros que permitan el mejor cumplimento de las actividades en cada sitio de trabajo y que se encuentran apoyadas por las TIC dentro de la organización.

- Fomentar la cultura del adecuado uso de los recursos tecnológicos al interior del INVISBU.
- Establecer lineamientos claros con respectos a las TIC que garantice el adecuado funcionamiento de los procesos y del buen uso de los activos de información al interior del Instituto.

## ALCANCE

Las políticas y lineamiento establecidos en este manual aplican para todos los usuarios del Instituto de Vivienda Interés Social y Reforma Urbana del Municipio de Bucaramanga – INVISBU en ejercicio de sus funciones, que se apoyan y que interactúan con la infraestructura de las tecnologías de Información y la Comunicación.

## NORMATIVIDAD

- La Constitución Política de Colombia.
- La Ley 715 de 2001.
- La Ley 1341 del 30 de julio de 2009.
- Ley 1581 de 2012 Protección de datos personales.
- Ley 1712 de 2014 Por medio de la cual se crea la Ley de Transparencia y del Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Decreto 1078 de 2015 Titulo 9 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
- Decreto 415 de 2016 "Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones".
- Circular 001 de 2017 Superintendencia de Industria y comercio - Por medio de la cual se imparten instrucciones a los Responsables y Encargados del tratamiento de datos personales respecto de la transferencia y transmisión de datos a terceros países.
- Decreto 1413 de 2017 "Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título 111 de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales".
- Ley 1928 de 2018 Por medio de la cual se aprueba el "Convenio sobre la ciberdelincuencia" adoptado el 23 de noviembre de 2001, en Budapest.
- Decreto 1125 de 2018 Por el cual se modifica el numeral 2 del artículo 2.2.8.4.4 del Decreto número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1008 de 2018 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".

## DEFINICIONES

Las definiciones están relacionadas con las TIC y el entorno en el que se mueven el INVISBU.

**Access Point o Punto de acceso inalámbrico**: (WAP o AP por sus siglas en inglés: Wireless Access Point) En una red de computadores, es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Normalmente un Access Point también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos.

**Administrador de Red: .**Es la persona encargada de la administración de la red.
Entre sus actividades incluye la administración, mantenimiento y monitoreo de los Equipos de comunicaciones y servidores que conforman la red: switches, routers, firewalls, entre otras.

**Amenaza:** Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio.

**Ancho de banda**: Nos indica la capacidad de comunicación, o la velocidad de transmisión de datos de una línea de conexión.

**Antispam:** Antispam es un producto, herramienta, servicio o mejor práctica que detiene el spam o correo no deseado antes de que se convierta en una molestia para los usuarios. El antispam debe ser parte de una estrategia de seguridad multinivel.

**Antivirus:** Antivirus es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

**Base de Datos: (Data Base).** Conjunto de datos relacionados que se almacenan de forma que se pueda acceder a ellos de manera sencilla, con la posibilidad de relacionarlos, ordenarlos en base a diferentes criterios, etc. Las bases de datos son uno de los grupos de aplicaciones de productividad personal más extendidos.

**Chat**: Comunicación simultánea de dos o más personas a través de Internet. Hasta hace poco tiempo sólo era posible la "conversación" escrita, pero los avances tecnológicos permiten ya la comunicación audio y video.

**Cifrado**: un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo. Letras que representan notas o acordes.

**Cookies:** o **galleta informática** es una pequeña información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del usuario.

**Copia de seguridad** Salvaguarda del sistema o de datos en un momento concreto, que permite recuperar esos datos o el sistema en el estado en que se encontraban en el momento de realizarla. También hace referencia a todo aquello que permite reemplazar a un elemento defectuoso. El término se refiere comúnmente a la realización de copias de seguridad de ficheros y programas con un software especial: los programas de copias

de seguridad. Es muy conveniente utilizar estos programas de vez en cuando para guardar en lugar seguro los datos más importantes para prevenir pérdidas de información debidas a posibles fallos del sistema.

**Contraseña de Usuario:** Una contraseña de usuario o clave es una forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña normalmente debe mantenerse en secreto ante aquellos a quien no se le permite el acceso. Aquellos que desean acceder a la información se les solicitan una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso.

**Correo electrónico:** (en inglés: *e-mail*), es un servicio de red que permite a los usuarios enviar y recibir mensajes (también denominados mensajes electrónicos o cartas electrónicas) mediante sistemas de comunicación electrónicos

**Encriptación**: La encriptación es un método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden es cifrar y utilizar los datos.
A veces, el malware utiliza la encriptación para ocultarse del software de seguridad. Es decir, el malware cifrado revuelve el código del programa para que sea difícil detectarlo.

**Firewall**: Mecanismo de seguridad en Internet frente a accesos no autorizados.

**Hacker:**se refiere a la acción de explorar y buscar las limitantes de un código o de una máquina.Según el "Glosario del Argot Hacker" o "Jargon File", cuyo creador fue Eric S. Raymond, el término hacker también significa acción de irrumpir o entrar de manera forzada a un sistema de cómputo o a una red. Este último significado para muchos hace alusión al término crackear. Sin embargo, en The New Hacker's Dictionary se plantea como un significado igualmente válido para hackear.

**Hub**: es el dispositivo que concentra los cables de una red local.

**Infraestructura:** Conjunto de elementos o de servicios básicos para la creación y el funcionamiento de una organización o entidad.

**IpAddress (Dirección IP):** Dirección de 32 bits definida por el Protocolo de Internet. Se representa usualmente mediante notación decimal separada por puntos. Un ejemplo de IpAddress es: 192.168.1.250.

**Intranet:** Red propia de una organización, diseñada y desarrollada siguiendo los protocolos propios de Internet; en particular el protocolo TCP/IP. Puede tratarse de una red aislada, es decir, no conectada a Internet.

**IP (Internet Protocol):** Protocolo principal de comunicaciones a través de Internet. La transmisión de información ocurre mediante pequeños paquetes de “bits” que contienen la información que está siendo enviada y la dirección hacia la que se dirigen.

**ISP:** (Internet ServiceProvider) (Proveedor de servicios de Internet): La institución que ofrece la conexión a Internet.

**Log:** es un registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y porqué (who, what, when, where y why) un evento ocurre para un dispositivo en particular o aplicación.

**Logging o registro histórico de actividades:** como su nombre lo dice es un registro de las actividades en un sistema de información o aplicación, el cual permite analizar la trazabilidad de los mismo.

**Modem:** Equipo utilizado para adecuar las señales digitales de una computadora a una línea telefónica o a una ISDN, mediante procesos denominados modulación (para transmitir información) y demodulación (para recibir información).

**Password:** *«Password» redirige aquí. Para otras acepciones, véase Password (desambiguación).* Utilización de una contraseña en Wikipedia. Una **contraseña** o **clave** es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quien no se le permite el acceso. A aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso.

**PDF (Portable Document Format):** El formato utilizado por el Acrobat de Adobe para representar documentos de manera independiente al sistema operativo en que fueron creados. Los archivos *.PDF pueden incluir texto y gráficas; además de poder ser representados en diferentes computadoras y sistemas operativos. Para poder ver un documento *.PDF, es necesario utilizar el Acrobat de Adobe Systems.

**Política de Seguridad Informática:** Es una forma de comunicarse con los usuarios y los gerentes. Las PSI establecen en canal formal de actuación del personal, en relación con los recursos y servicios informa 'ticos, importantes de la organización.

**Protección heurística (Heuristics-BasedProtection):**Forma de tecnología antivirus que detecta las infecciones mediante el escrutinio de la estructura general de un programa, las instrucciones de sus computadoras y otros datos contenidos en el archivo. Una exploración heurística hace una evaluación sobre la probabilidad de que el programa sea malicioso con base en la aparente intención de la lógica.
Este plan puede detectar infecciones desconocidas, ya que busca lógica generalmente sospechosa, en lugar de huellas específicas de malware, tales como los métodos tradicionales de antivirus de firmas. La protección heurística debería hacer parte de una estrategia de seguridad estándar de múltiples niveles.

**Rauter**: es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

**Red:** Una red de computadoras, también llamada red de ordenadores o red informática, es un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.), servicios (acceso a internet, e-mail, chat, juegos).

**Red de datos:** Se denomina red de datos a aquellas infraestructuras o redes de comunicación que se ha diseñado específicamente a la transmisión de información mediante el intercambio de datos.

**Seguridad Informática**: o seguridad de tecnologías de la información es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante.

**Sistemas de Control Interno:** es dentro de la empresa un seguimiento y control de las actividades que se realizan en el seno de la misma. Corrigen errores y se asegura del cumplimiento de los objetivos. Cada área funcional de la empresa presentara un control interno de sus actividades. Estos sistemas de control buscan que la empresa tenga una mejor eficiencia.

**Sistema de Información**: es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

**Software dañino, maligno o nocivo**: toma su nombre del término "software Malicioso" y es diseñado para entrar en el sistema de su computadora para causar un daño significativo sin su conocimiento y menos con su consentimiento.

**Riesgo informático**: La posibilidad de que una amenaza se materialice, utilizando vulnerabilidad existentes de un activo o un grupo de activos, generándole pérdidas o daños.

**Roaming**: acceso a Internet desde diversos lugares del mundo, al precio de una llamada local.

**Router**. Ruteador. Sistema constituido por hardware y software repara la transmisión de datos en Internet. El emisor y el receptor deben utilizar el mismo protocolo

**Sistemas de Información:** Es el conjunto de procedimientos, personas y equipos capaces de recibir datos y producir información.

**Sistema Operativo:** El software de nivel bajo que se encarga de organizar la operación de la computadora, asignar recursos, manejar la interfaz de los diversos periféricos, y comunicarse con el usuario. El sistema operativo es el software más importante de un computador, ya que sin él la operación del computador sería imposible. Algunos de los sistemas operativos más comunes son: Windows, MSDOS, MacOS, Linux y Solaris.

**Spam:** Es cualquier mensaje destinado a una audiencia general (o sea, un comunicado de masas) que se envía a la gente por e-mail sin que lo soliciten. Generalmente las direcciones a las que llegan esos mails son robadas y la mayoría de las veces esos mails son publicidad o contiene algún virus. Representa una violación a la privacidad del usuario.

**Swiches**: es un dispositivo analógico de lógica de interconexión de redes de computadores que opera en la capa 2.

**TI:** Tecnología Informática.

**TIC**: Tecnologías de la Información y las Comunicaciones.

**Toolkit:**Paquete de software diseñado para ayudar a los hackers a crear y propagar códigos maliciosos. Los toolkits frecuentemente automatizan la creación y propagación de malware al punto que, incluso los principiante delincuentes cibernéticos son capaces de utilizar amenazas complejas. También pueden
utilizarse toolkits para lanzar ataques web, enviar spam y crear sitios de phishing y mensajes de correo electrónico.

**Usuario**: *«Usuario» redirige aquí. Para otras acepciones, véase Consumidor.* Según la Real Academia Española, un **usuario** es «aquél que usa algo» o «que usa ordinariamente algo». 1 En informática este término se utiliza con especial relevancia.

**Usuario final**: En informática, el término **usuario final** designa a la persona o personas que van a manipular de manera directa un producto de software.

**Vulnerabilidad:** Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad (CIA) de los sistemas. Las vulnerabilidades pueden hacer lo siguiente:

- Permitir que un atacante ejecute comandos como otro usuario
- Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos
- Permitir a un atacante hacerse pasar por otra entidad
- Permitir a un atacante realizar una negación de servicio

**Virus:** Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario. Un virus debe cumplir con dos criterios:

- Debe ejecutarse por sí mismo: generalmente coloca su propio código en la ruta de ejecución de otro programa.
- Debe reproducirse: por ejemplo, puede reemplazar otros archivos ejecutables con una copia del archivo infectado por un virus. Los virus pueden infectar computadores de escritorio y servidores de red.

**Web**: es un vocablo inglés que significa **"red"**, **"telaraña"** o **"malla"**. El concepto se utiliza en el ámbito tecnológico para nombrar a una red informática y, en general, a **Internet** (en este caso, suele escribirse como **Web**, con la W mayúscula).

**Web 2.0:** El término Web 2.0 comprende aquellos sitios web que facilitan el compartir información, la interoperabilidad, el diseño centrado en el usuario y la colaboración en la World Wide Web.

**POLITICAS GENERALES (Usuario Final y Administrador)**

- ✓ Los recursos y servicios de Tecnología de Información y Comunicaciones (TIC) suministrados por el INVISBU a los funcionarios de las diferentes áreas de la entidad, deberán ser para el estricto uso en actividades propias o directamente relacionadas con las funciones del trabajo que desempeñan.
- ✓ Es responsabilidad de la directiva de la organización garantizar los recursos necesarios para el mantenimiento, la operación y la actualización de los recursos, servicios e infraestructura TIC de la organización.
- ✓ La asignación de recursos y el uso de los servicios TIC estarán sujeta a la aprobación de presupuesto de la cada vigencia.
- ✓ Todos los computadores de trabajo deberán disponer de un sistema operativo legal que solamente permita el acceso a los recursos de la red e internet con el uso de un nombre de usuario y una contraseña.
- ✓ Todos los computadores de trabajo deberán disponer de una licencia que permita el uso de cualquier aplicación que así lo amerite.
- ✓ Los servicios y recursos TIC deberán ser administrados por personal técnico del área de sistemas, quienes tendrán la responsabilidad de mantener, configurar, modificar, instalar y actualizar los servicios; los cuales siempre deberán estar alineados con las políticas y lineamientos de la Institución.
- ✓ Para los servicios que se prestarán a los usuarios internos de la entidad se deben tomar en cuenta las siguientes consideraciones:
    - Será deber de los usuarios de distintas áreas respetar y hacer respetar las políticas y lineamientos consignados en este manual.
    - Será deber de las áreas informar a sus usuarios sobre la presente normativa.

**Usuario Final**

- Las autorizaciones concedidas a los usuarios para acceder a los recursos de la red serán rigurosamente individuales y no transferibles. Las mismas pueden acabarse con la interrupción de las actividades que la han justificado.
- Todo servicio o soporte deberá ser solicitado al personal de sistemas; el cual analizara y priorizara de acuerdo su nivel de importancia y necesidades para la solución.
- Todos los usuarios deben cumplir las políticas y lineamientos relacionados la tecnología de información que manejen.

**Usuario Administrador**

- El acceso a los servicios de la red será administrado por el personal del área de Sistemas en función de las necesidades y prioridades de la Institución y de la disponibilidad de recursos.
- Las competencias y responsabilidades del personal de sistemas que serán los encargados de administrar los servicios; deberán estar claramente explícitas en la descripción de sus funciones y procedimientos internos asociados.
- En los servicios que lo ameriten, se deberá utilizar un nombre de usuario (ID) Único (administrador) de manera de se pueda identificar, controlar y mantener su responsabilidad. La Implementación de nuevos servicios de carácter innovador o de mejora, deberá ser realizada en ambientes de prueba con la finalidad de evitar cualquier impacto negativo sobre la red.
- La Implementación de nuevos servicios deberá ser realizada en ambientes de prueba con la finalidad de evitar cualquier impacto negativo sobre los servicios y el correcto funcionamiento de la infraestructura tecnológica.

- El administrador del servicio definirá los acuerdos de servicio, divulgarlos a su comunidad y respetarlos para dar cumplimiento a la prestación de dicho servicio de forma oportuna y correcta.
- Para identificar los usuarios, grupo de usuarios, equipos asignados en la Red de Datos del INVISBU se debe tomar en cuenta el documento protocolo de lineamientos elaborado para su definición e identificación de los mismos.
- Para llevar un registro y control de la información de los equipos administrados, se debe considerar el mantenimiento de la hoja de vida de los equipos de computador de la entidad

**Documentación Asociada:**

- PETI
- Hoja de vida de los equipos de computador
- Lineamientos Creación de Usuarios INVISBU
- Formato Orden de Servicios de Sistemas INVISBU

## POLÍTICA DE SEGURIDAD FÍSICA Y MEDIO AMBIENTE

➢ **Red regulada**

La infraestructura de la red eléctrica regulada deberá desarrollarse siguiendo las normas y estándares para este fin, permitiendo la seguridad del recurso humano, tecnológico, documental y de activos d información del INVISBU. De la misma manera, deberá asegurar el servicio, la protección de la información y de los equipos en todas las áreas de trabajo.

❖ **Inventario de UPS**

El inventario de los equipos electrónico UPS permitirá identificar la cantidad de equipos existentes, su estado, la última fecha de mantenimiento preventivo, el área que cubre y las área que faltan, por lo cual deberá:

- Solicitarse el mantenimiento prevenido anual o semestralmente con personal técnico expertos para garantizar la vida útil de los equipos y el respaldo que brindan en la institución.
- Actualizar el inventario cada que se realizase una actividad que lo alimente.
- Solicitar la regulación eléctrica de las áreas pendiente en la institución.

❖ **Mantenimiento UPS**

Durante el mantenimiento de las UPS, tener presente:

- Estado general de la UPS (Batería). Para evaluar el tiempo de vida.
- Verificar el sello de garantía en los equipos después del mantenimiento.
- Probar el funcionamiento general de la UPS.

❖ **Responsabilidades**

Los diferentes usuarios de las áreas que están reguladas con una infraestructura eléctrica deben cumplir varias responsabilidades para garantizar la protección de la información que manejan y de los equipos, las cuales son:

- Los usuarios de las zonas reguladas eléctricamente deberán verificar que el equipo de cómputo en su responsabilidad este conectados al toma naranja (CPU y Pantalla).
- Los usuarios deben verificar que las impresoras, ventiladores, radios entre otros que No sean equipos de cómputo No estén conectados a tomas naranja.

- El usuario No deberá conectar cortapicos o reguladores a toma naranja para tratar de conectar más equipos.

➢ **Red de Datos**

El INVISBU cuenta con infraestructura de red que comprende el Rack de comunicaciones, el cableado, swiches, Access Point, routers, firewall, DVR, sistema inalámbrico que permite la interconexión de equipos (computadores, impresoras) para el servicio de acceso a Internet, interacción entre usuarios a través de sistemas de información entre otros.

El área de Sistemas es la encargada de garantizar el funcionamiento de estos servicios, para lo cual realiza verificación permanente de los recursos de red existentes, mejoras que pueda realizarse y servicios externos que puedan ayudar en el soporte y monitoreo.

**Centro de cableado, Rack de Comunicaciones o centro de computo**

El centro de cómputo es el lugar o sitio físico único donde se concentra el cableado de la red local y se conectan los dispositivos que permiten la interconexión para la comunicación interna y hacia internet. En este sitio solo está permitido el acceso al personal de soporte técnico y de sistemas de la entidad o personas externas autorizadas que cumplan una labor contratada, para los diferentes usuarios internos está restringido el acceso.
El centro de cableado es el espacio donde se organiza el cableado, se ubican los dispositivos, DVR, Firewall, servidores, router, transiver y demás que permitan la interconexión para el funcionamiento de la red local, estos al ser cerrados permiten brindar seguridad y protección contra el medio ambiente.

➢ **Equipos**

**Inventario de equipos**

Los equipos de cómputo de la organización son los activos indispensables para la interacción tecnológica en el INVISBU y para el control general debe tener:

- Usuario responsable del equipo.
- Código Inventario asignado
- Dirección Ip.
- Registro y mantenimiento de la hoja de vida
- Registro de Observaciones Generales

Actividades relacionadas con el registro de equipos:

- Cada que ingrese un equipo nuevo debe registrarse en el inventario
- Cada que el equipo cambie de usuario debe actualizarse el inventario
- Cantidad de equipos por sistema operativo
- Cantidad de equipos por licenciados y no licenciados

**Protección y ubicación de los equipos de cómputo**

Los usuarios internos no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del Jefe Inmediato

(si es cambio de ubicación), Almacén (si es descarga del inventario) y área de Sistemas será la que haga el traslado, debiéndose solicitar servicio por escrito.

- El equipo asignado, deberá ser para uso exclusivo de las funciones institucionales encomendadas por la entidad o relacionadas con el cargo.
- Será responsabilidad del usuario interno solicitar al jefe inmediato la capacitación necesaria para el manejo de las herramientas informáticas entre otras instaladas y autorizadas en los equipos que utilizan, a fin de evitar riesgos por mal uso.
- Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos, a menos que sea en botellas de plástico.
- Se debe mantener el equipo informático en un entorno limpio y sin humedad.
- El usuario interno debe asegurarse que los cables de conexión no sean pisados o aplastados al colocar otros objetos encima o contra ellos.
- El personal autorizado para llevar a cabo el servicio y las reparaciones es el del área de sistemas o personal externo con permiso.
- Los usuarios internos deberán asegurarse de respaldar la información que considere relevante cuando se le haga su mantenimiento preventivo o reparación alguna.
- En caso de robo o desaparición del equipo asignado; el usuario interno deberá dar aviso al subdirección administrativa.

**Mantenimiento preventivo**

- Elaborar el cronograma anual para la programación del mantenimiento preventivo de los equipos de cómputo.
- Notificar por correo con antelación a cada usuario la fecha y hora del mantenimiento.
- Llevar el registro y control del mantenimiento realizado semestralmente.
- Elaborar el indicador trimestral del mantenimiento.
- Tener en cuanta en el PETI el análisis de los equipo.
- Elaborar el informe de baja de cada equipo cuando se requiera.
- Antes del mantenimiento explicar a cada usuario como debe hacer y donde la debe hacer la copia de seguridad de su información porque es el responsable del manejo la información.
- Brindar soporte técnico correctivo del equipo cuando el usuario lo requiera.
- Al entregar el equipo con el mantenimiento preventivo realizado, solicitarle al usuario la verificación del funcionamiento general del equipo, así como de la información.

**Seguridad de los equipos: protección contra virus**

Para la instalación de software antivirus informático, se debe:

- Revisar la capacidad de los equipos, antes de la instalación.
- Ejecutar pruebas de funcionamiento una vez instalado.

**Daño de equipos**

El equipo de cómputo o cualquier recurso de soporte TIC que sufra alguna daño por maltrato, descuido o negligencia por parte del usuario comprobada, deberá ser reportado a la Subdireccion administrativa y financiera para que tome las acciones pertinentes en estos casos.

**Seguridad en el área de trabajo**

- El área del centro de cómputo debe ser un lugar restringido y solo el personal autorizado podrá acceder a él.

- Estos sitios en donde se encuentran elementos de TIC, como servidores, Rack de comunicaciones, UPS, Firewall, etc., se recomienda tener un aire acondiciona que le garantice una temperatura adecuada.
- Solo los técnicos del área de sistemas deberán tener acceso a la herramienta, partes y equipos en reparación.
- No deben repararse, ni mucho menos cambiar partes a equipos que no sean institucionales.
- El mantenimiento preventivo y correctivo solo se realizara a equipos institucionales.

➢ **Software**

**Respaldo y recuperación:** Es la una labor que se debe llevar acabo al interior de la organización con el fin de garantizar la continuidad del procesamiento de los datos de las aplicaciones que se manejan

**Protección y respaldo de la información**

El propósito es determinar el estado actual de protección de la información en la entidad y plantear estrategias para proteger y facilitar su utilización de acuerdo a las necesidades.

En este documento se definen los parámetros que deberán seguirse al interior de la organización para el almacenamiento y recuperación de la información en el corto y largo plazo, así como de la recuperación de la información guardada a nivel de medios de almacenamiento para responder a los requerimientos de los procesos de la entidad. Estos parámetros deberán ser atendidos por los diferentes usuarios internos que hacen parte del INVISBU.
El mayor activo de cualquier organización es la información, por tal razón se deben crear procedimientos que garanticen el apropiado uso de la información y su correcta disponibilidad. Además velar por su Seguridad, Confidencialidad, Integridad y Disponibilidad.

La información de la entidad deberá mantenerse disponible a las personas que la requieran.

La organización deberá identificar mecanismos que permitan que las actividades de respaldo y recuperación sean adecuadas.

Los niveles de protección y clasificación determinados para la seguridad de la información deberán mantenerse en todo momento. (Acceso, toma de respaldo, backup, transporte, recuperación, otros).

Se deben mantener las medidas y controles establecidos para la protección de la información.

Los usuarios del INVISBU son responsables de la información institucional que manejan. Durante el mantenimiento preventivo se realiza una copia, la cual se debe conservar y guardar una copia de respaldo en otro sitio i/o dispositivo.

- Los usuarios respaldan y protegen la información que manejan, con medidas y lineamientos que eviten accesos de personas no autorizadas.

- El archivo central de la entidad deberá guardar los respaldos digitales de la información de gestión e históricos en sitios adecuados para la preservación que permitan la continuidad y que estén acorde a lo establecido en las tablas de retención documental.
- El área de Sistemas es la responsable del respaldo y seguridad de las bases de datos a las que tenga acceso y deberá tener copia en varios espacios como garantía de continuidad de la organización.
- La entidad deberá tener contratada legalmente el espacio fuera de sus instalaciones para el respaldo de las bases de datos y otra información clasificada como relevante.
- Los usuarios internos deberán seguir los procedimientos de respaldo de la información y crear inventario de copias de la información de los medios donde se haya guardado la información local y enviada al archivo central, para facilitar el seguimiento de la actividad de seguridad y restauración.

**Adquisición**

La solicitud de las necesidades las TIC entre ellas la adquisición de Software se debe analizar y requerir por medio del Plan Estratégico de Sistemas anual.

- **Licencias del Software**
  El área de sistemas velara porque todo el software que se instale en los equipos de la organización sea licenciado.
- **Control de Acceso Físico**
  Estos son los permisos relacionados con el acceso físico a las áreas restringidas (Centro de Computo) y sitios confidenciales.

## POLÍTICA DE SEGURIDAD DE LA RED

- El objetivo de esta política es especificar la normatividad de seguridad de la red del INVISBU y que obedezca a la confidencialidad, integridad y disponibilidad de la información en los usos requeridos por los usuarios tanto internos como externos.
- Las IP, topologías, configuraciones e información relacionada con el diseño de las redes y seguridad la entidad deberán ser tratadas como información confidencial.
- Todas las conexiones a redes externas en tiempo real que accedan a la red Interna de la organización, deberán pasar a través del firewall previamente parametrizado con las políticas de navegación incluyendo antivirus de red, verificación de datos, detección de ataques, detección de intentos de intrusión, administración de permisos de circulación y autenticación de usuarios, y bloqueo de sitios o intrusos.
- Todo intercambio electrónico de información o interacción entre sistemas de información con entidades externas deberá estar soportado con un acuerdo o documento de formalización.

La información es un elemento esencial en la gestión del instituto, actualmente la información se maneja a través de sistemas de información en la red a nivel interno y externo. Por tal motivo, están expuestos a riesgos de seguridad, donde puede darse el acceso no permitido a la información para hacer daño. Entre las vulnerabilidades más relevantes esta “las puertas invisibles” descubiertas en los sistemas operativos,

aplicaciones de software, browsers de Internet, protocolos de red, correos electrónicos y diferentes servicios informáticos. Se hace necesaria para garantizar la continuidad de las operaciones de la entidad, identificando sus amenazas.

Entre los equipos de seguridad informática y protecciones que existen o que se recomiendan se tienen:

- **Cortafuegos (firewall)**

  En un Dispositivo con gran tecnología que combinando hardware y software basado en uso de circuitos integrados de aplicación específica, brinda seguridad perimetral realizando control sobre el tráfico de las redes en tiempo real, garantizando protección completa a los sistemas de información que navegan en la red.

  El nivel de seguridad que ofrece es muy alto, para lo cual presenta varias alternativas de solución de seguridad en la red como es el permiso de terceros para navegar en la red de forma controlada, la restricción en la navegación a los usuarios internos, la configuración de antivirus para servicios en la red, control del ancho de banda, control de acceso, entre otros igualmente importantes.

- **Servidores**
  Para garantizar la seguridad de la información en el instituto, la gestión interna administrativa y financiera se debe velar porque los servidores manejen el volumen de gestión alto y estén en sitios dentro de la institución adecuados.
  Los servidores (Web, BD, Aplicaciones, entre otros.), si se recomiendas que estén en sitios externos ideales y con la seguridad correspondiente (firewall y políticas de navegación especiales).

- **Aplicaciones de Usuario**
  Para prevenir la vulnerabilidad en las aplicaciones locales y de internet en los equipos de los usuarios internos, se deben tomar medidas de acuerdo al tipo de software, poniendo en marcha otra clase de protecciones; como el antivirus corporativo, antivirus de red, administración de los usuarios donde se determine el acceso y las restricciones pertinentes, entre otras soluciones que permitan reducir el posible riesgo.

- **Protección física y digital de la información**
  Con la finalidad de evitar riesgos potenciales a los activos de información de la entidad que maneja el usuario interno, relacionados con su operar cotidiano, ya sean de manera accidental o intencionada, que puedan ocasionar la interrupción total o parcial, de las actividades. En este documento se disponen lineamientos que deberán adoptarse al interior de la organización para la protección de la información, tanto física como digital y con acceso a través de los computadores, estas políticas deberán ser aplicadas por todos los usuarios externos y cada una de las áreas implicadas.
  Para el INVISBU es de vital importancia proteger toda información sensible, evitando que sea conocida por personas diferentes a aquellas que la requieren o que sea publicada de manera indistinta. Por tanto los usuarios externos deberán cumplir:

- Los usuarios dueños de la información son responsables, mientras tengan la información bajo su control, de mantener los niveles de protección y clasificación establecidos para la misma en todo momento, haciendo uso adecuado de los recursos a su disposición.
- Es responsabilidad de los usuarios el identificar riesgos relacionados al disponer de la información en su puesto de trabajo e iniciar las acciones para mitigarlos.
- Es responsabilidad de cada usuario la protección de la información a cargo, por lo que debe mantener presente NO publicar o dejar a la vista, documentos o datos confidenciales, delicados, confidenciales, por ejemplo: Nombre de Usuario y Password, Contratos, Listas de Clientes, Propiedad Intelectual, Datos de Funcionarios

- Los usuarios del INVISBU deberán tomarse el tiempo necesario antes de abandonar la oficina para recoger y asegurar el material confidencial. (Portátiles, tables, Memorias USB, entre otros.).

Cada usuario de la entidad para mantener su computador bajo control, deberá bloquear la sesión al alejarse de su computador, aunque sea por poco tiempo, minimizando el tiempo que el equipo quedaría sin control ya que cualquier ausencia puede extenderse.

- **Protección contra software maligno y uso del Internet**

En este ítem se mencionan aspectos de control que van a permitir mitigar riesgos generados por el acceso a Internet y a redes públicas, el intercambio de medios de almacenamiento removibles, el intercambio de información con instituciones externas, entre otras, los cuales exponen los sistemas la entidad a la propagación interna y externa de software con código malicioso o nocivo, comprometiendo directamente la integridad, la disponibilidad y la confidencialidad de la información procesada por cada uno delos componentes de la red.

El INVISBU con el objetivo de facilitar la realización de labores diarias de cada usuario interno, da acceso a Internet; para los cual dicho servicio se ampara en las políticas y lineamientos expuestos en este documento. Por todo esto se hace necesario la publicación y socialización de estas políticas a todo el personal que trabaja con el Instituto.

- Cualquier usuario que tenga sospecha de una infección por un virus debe llamar al personal de soporte de Sistemas para que ellos hagan las gestionen para la prevención y eliminación del virus del computador.
- Los usuarios no podrán bajar software desde cualquier sistema fuera de la red de la organización.
- Los usuarios No deben utilizar archivos obtenidos externamente desde Internet o de una persona u organización diferente a los distribuidores confiables o conocidos, a menos que el software haya sido examinado y revisado por un antivirus.
- Antes de ser descomprimido, todo archivo transferido desde sistemas externos al instituto, debe ser analizado con un sistema antivirus aprobado.

- Los usuarios intencionalmente no deben escribir, generar, compilar, copiar, almacenar, propagar, ejecutar o intentar introducir cualquier código de computador diseñado para auto replicarse, deteriorar o que dificulte el desempeño de cualquier sistema de la organización.
- Los usuarios del Internet deberán abstenerse de visitar espacios en la Web o sitios que afecten la productividad de la institución.
- Se deberá evitar el acceso desde el espacio institucional a sitios relacionados con la pornografía y fundamentalmente si éste involucra a menores de edad. Igualmente, se prohíbe la descarga y uso de software malicioso o documentos que brinden información sobre cómo atentar contra la seguridad de la información institucional.
- Los Empleados deberán abstenerse de brindar cualquier tipo de información de la entidad en sitios no autorizados o que no cuenten con mecanismos de seguridad que garanticen la confidencialidad de la información en tránsito.
- Los usuarios internos de la organización No deben comprar bienes o servicios a través de Internet a nombre del INVISBU.
- Los usuarios, deben evitar descargar y/o emplear archivos de imagen, sonido o similares que puedan estar protegidos por derechos de autor de terceros sin la previa autorización de los mismos.
- Los usuarios no deben instalar software en sus computadores de trabajo, incluso si este software es libre o no licenciado; toda instalación de software debe hacerla un técnico autorizado (área de Sistemas).
- Los usuarios deben estar conscientes de que toda la información (incluida la de navegación) que transite por la red de la entidad, por ser para la labor diaria es propiedad de la misma y por ende puede ser monitoreada con objetivos de administración, seguridad o auditoría por personal autorizado de la institución.
- Los usuarios del Internet deben estar conscientes de que este, solamente deben ser utilizados para propósitos lícitos y en cumplimiento de las funciones específicas de su cargo.
- El personal del instituto no debe utilizar el sistema de navegación por internet para participar en grupos de discusión en Internet, listas de Correo, chats o cualquier otro foro público, a menos que su participación sea meramente con fines institucionales.
- El INVISBU facilita el acceso al uso de medios electrónicos para comercio electrónico como el pago de facturas, transacciones bancarias de sus funcionarios y lectura de correos personales que tengan acceso vía web, pero no asume ninguna responsabilidad por estas, ni recomienda el uso. Si el usuario hace uso de estos servicios de todas maneras asume que puede ser monitoreada toda la información que de este uso se derive como si fuese de la institución misma.

## POLÍTICA DE SEGURIDAD DE INFORMACIÓN

La política de seguridad es un documento de alto nivel que denota el compromiso de la dirección de la entidad con la seguridad de la información.

Esta política nace como una necesidad de la organización para concientizar a los usuarios internos que hacen uso de los sistemas de información; aquí se describirá la protección y el funcionamiento para la utilización adecuada.

Teniendo en cuenta que la información es el activo más preciado de las empresas y entidades en general; se hace necesario tomar todas las precauciones, para mantener y preservar información, para ello el INVISBU debe saber que los elementos a tener en cuenta serán los siguientes: confidencialidad, disponibilidad, privacidad, control, auditoria, autenticación e integralidad. Así como adoptar buenas prácticas en cuanto a la gestión y administración de las Tecnologías de la Información.

En general la Política de Seguridad de la Información es la declaración general que representa la posición de la dirección, con respecto a la protección de los activos de información (los funcionarios, la información, los procesos, las tecnologías de información incluido el hardware y el software), a la implementación del Sistema de Gestión de Seguridad de la Información y al apoyo, generación y publicación de sus políticas, procedimientos e instructivos. El INVISBU para el cumplimiento de su misión, visión, objetivo estratégico y apegado a sus valores corporativos, establece la función de Seguridad de la Información en la Entidad, con el objetivo de:

a) Disminuir el riesgo en las funciones más importantes y críticas de la entidad.
b) Dar cumplimiento a los principios de seguridad de la información.
c) Cumplir con los principios de la función administrativa.
d) Mantener la confianza de sus clientes internos y externos.
e) Apoyar la innovación de las TIC.
f) Poner en marcha un sistema de gestión de seguridad de la información ajustado a las necesidades y dimensión de la entidad.
g) Proteger los activos tecnológicos y de información de la organización.
h) Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información. Fortalecer la cultura de seguridad de la información al interior de la organización.
i) Garantizar la continuidad del negocio frente a incidentes.

Esta política va dirigida al que? al cómo? y cual el la protección a establecer; para lo cual se apoya en las siguientes políticas:

- **Política de seguridad de los Sistemas de Información**

  El propósito de esta política es establecer límites que resguarden la información de ser liberada (deliberada o no deliberadamente) a las personas erradas.

  En el INVISBU la Información es un activo esencial para la prestación del servicio y la toma de decisiones, por lo cual existe un deber manifiesto de salvaguardar la propiedad más relevante como estrategia orientada a la continuidad del negocio, la administración de peligros y el fortalecimiento de la cultura de seguridad.

  - Dentro de esta política se normalizara la protección de los activos de la información los cuales serán identificados, clasificados y socializados, con el fin de establecer los elementos de protección necesarios.

  - La organización a través del personal de las TIC, definirá y pondrá en marcha controles para proteger la información; los cuales garantizaran su disponibilidad.

- Todos los funcionarios de la institución incluyendo los contratistas, serán responsables de proteger la información a la cual tienen acceso para evitar riesgos (pérdida, alteración, uso indebido o destrucción).
- Se deberán programar seguimientos y controles a los sistemas de información existentes en el instituto.
- Solo se permitirá software que se haya adquirido legalmente y el software libre que brinde seguridad y soporte.
- Todos los usuarios, como responsabilidad sobre la seguridad de la información, deberán comunicar los riesgos que identifique.
- El incumplimiento de las políticas serán notificadas, reconocidas y monitoreadas.
- El INVISBU en cabeza del personal de las TIC, deberá elaborar un plan de continuidad de las actividades de la Institución ante eventos que puedan ocurrir.

➢ **Seguridad del comercio electrónico**

Esta política tiene como objeto prevenir la revelación de información privada, el fraude en contra o en nombre de la entidad, la privacidad de la información de cuentas y la seguridad de las transacciones realizadas a través de Internet o redes externas.

Toda información acerca de pagos, como números de cuentas corrientes entre otras, debe ser acordada su transmisión con el banco a través de firmas digitales asignada al responsable de la actividad y con el cumplimiento de los protocolos de seguridad exigidos por la unidad de seguridad del ente bancario con el cual se establecen dichas transacciones.

➢ **Logging o Registro Histórico de Actividades (Logs de seguridad de aplicaciones confidenciales)**

En informática, se usa el término log, historial de log o registro, se refiere a la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos (eventos o acciones) que afectan a un proceso particular (aplicación, actividad de una red informática, etc.).

https://es.wikipedia.org/wiki/Log_(inform%C3%A1tica)

El fin de esta política es obtener registros de los movimientos que se realizan dentro de los sistemas de información del INVISBU, buscando evitar conductas no apropiadas y así poder minimizar riesgos de seguridad en el uso de mismos.

Todas las aplicaciones de producción deben tener logs que muestren cada modificación, incorporación y borrado de la información.

Los logs de procesos relevantes deben de proveer información suficiente para soportar auditorías y contribuir a la eficiencia y cumplimiento de medidas de seguridad.

El log debe revisarse por lo menos cada mes. Durante este período, el administrador del sistema y/o dueño de la información, se debe asegurar que éste no sea modificado, y cerciorarse de que no sea leído por

personal no autorizado. Estos aspectos son importantes para la corrección de errores, auditorías o huecos de seguridad.

Para evitar conductas inapropiadas, crear un sentido de responsabilidad del usuario, y permitir una administración adecuada de los sistemas, todas las actividades de los usuarios que afecten producción deben ser trazables desde el log.

Las aplicaciones y otros manejadores de Bases de Datos, deben tener logs para las actividades de los usuarios y estadísticas relacionadas a estas actividades que les permitan identificar y detectar alarmas de posibles problemas o mal uso, y que reflejen eventos misionales de la institución sospechosos.

Todos los sistemas del INVISBU y todos los computadores conectados a una red deben tener un mismo horario y calendario adecuado, utilizando sincronía con los servidores, cuando sea posible. Esto para facilitar actividades de rastreo mediante los logs de los sistemas.

El manejo de Logs, los mecanismos para detectar y registrar eventos de seguridad significativos, deben ser resistentes a los ataques.

Los logs son una herramienta de gran valor que pueden ayudar a identificar y a solucionar muchas incidencias no contempladas.

**Bibliografía**


- ✓ https://es.wikipedia.org/wiki/Log_(inform%C3%A1tica)
- ✓ https://www.apc.org/sites/default/files/ICT_Policy_Handbook_ES.pdf
- ✓ Manual de Implementación de Políticas TIC, Escuela Nacional del Deporte, octubre de 2016
- ✓ Manual De Política De Tecnología E Información, Alcaldía mayor de Bogotá, agosto 2018


Elaboró: Javier Orlando Núñez Latorre – Asesor TIC INVISBU