INTRODUCCION

El presente documento tiene como objetivo ordenar el uso de los medios de información y comunicación en COMFABOY, abarca los servicios y recursos informáticos y los medios de comunicación.

1. POLÍTICAS DE SEGURIDAD SISTEMAS

1.1. SEGURIDAD FÍSICA

• Las áreas de sistemas deberán tener acceso restringido a personas no autorizadas, según el responsable del área, al igual que los cuartos de equipos y cuartos de UPS.
• Cuando la información es de acceso público e interno debe estar protegida por Firewalls, con esquema de seguridad, además de contar con medidas básicas de control del perímetro y también debe contar con sistemas de detección de intrusos.
• Todos los Trabajadores, deberán portar el carnet en un lugar visible, permitiendo con esto una mejor identificación y control de las personas que ingresan a las áreas de cómputo restringidas.
• Los bienes informáticos serán cargados al inventario del trabajador responsable y su movilización no se podrá realizar sin la aprobación de la dependencia que administre los bienes.
• Solo personal técnico autorizado por el responsable del área de sistemas de la entidad puede revisar, configurar y dar soporte a los bienes informáticos.
• Los Trabajadores de la Caja al usar los equipos de cómputo, se abstendrán de consumir alimentos, fumar o realizar actos que perjudiquen o pongan en riesgo el funcionamiento de los mismos o deterioren la información almacenada en los discos duros o medios magnéticos.
• El usuario no instalará ningún tipo de software estandarizado o no, shareware, freeware, demo, de dominio público, en los equipos sin la aprobación expresa de la JGSC, que debe solicitarse por escrito.
• Verificar la información que provengan de fuentes externas, a fin de corroborar que estén libres de cualquier agente externo que pueda contaminar o perjudicar el funcionamiento de los equipos.
• Mantener las pólizas de seguros de la tecnología de información en funcionamiento, incluyendo póliza colectiva de riesgos ante posibles pérdidas de información y daños irrecuperables en los medios de almacenamiento.
• En los tomacorrientes donde se alimenten los equipos de cómputo, no se deben conectar otros equipos que interfieran con el consumo de energía.
• Se debe propender por el uso de unidades ininterrumpidas de potencia UPS, para prevenir daños en los equipos ante ausencia de corriente.
• Debe existir medidas contra fuego, agua, y otras similares.

1.2. SEGURIDAD LÓGICA

• El usuario deberá cambiar periódicamente su clave de acceso de acuerdo a la criticidad de los sistemas de información que maneje.
• Todos los módulos de las aplicaciones que ingresen datos deberán tener una clave de acceso y establecer perfiles de usuarios para acceder a la información.
• Las palabras claves no deben aparecer en la pantalla al ser ingresadas, tampoco deben imprimirse o mantenerse en la máquina, y mucho menos en un medio que se encuentre en lugar visible.
• El administrador de la red y el administrador de la base de datos cambiará inmediatamente la clave de acceso a los empleados o contratistas que tengan ausencias definitivas de sus cargos o terminación de sus contratos. Para que esto sea posible, cada jefe de área o dependencia debe informar por escrito a la Jefatura del Grupo de Sistemas de Comfaboy sobre la novedad de personal, relacionando claramente los datos de los Trabajadores entrante y saliente.
• Cuando un usuario maneje aplicaciones específicas y sea removido de su puesto de trabajo de manera provisional o permanente, deberá hacer entrega formal del equipo a su cargo, las claves de acceso e instruir a su reemplazo en la utilización del software que administra, al igual que hacer entrega de la información relevante que estaba a su cargo.
• Es responsabilidad del área de soporte de la JGSC, proteger la información institucional que exista en los equipos en el evento que se vaya a realizar cambio de ellos.
• Todos los equipos susceptibles de infectarse con virus deberán estar dotados con antivirus permanentemente actualizados.
• Todo medio de almacenamiento que ingrese al sistema deberá ser previamente vacunado.
• Cualquier dependencia o área de la Caja del nivel Central o Local que reciba equipos de cómputo a través de comodatos o convenios ínter administrativos, deberá en coordinación con la “JGSC” cuidar que quede claramente establecido todo lo referente a seguros, mantenimiento preventivo y correctivo, licenciamiento de software, repotenciación y disposición final de los equipos.

1.3. RESPALDOS

• Los usuarios deberán respaldar en medios de almacenamiento flexible la información propia y relevante del disco duro de su equipo.
• Los usuarios deberán tener copias de la información propia y relevante de su labor en el servidor de respaldo o en el área de trabajo del servidor de la red que se haya destinado para este fin, respetando las cuotas de espacio asignadas para cada uno.
• Para efectos de brindar un adecuado servicio de soporte a los usuarios, y no poner en riesgo la información “institucional crítica”, cada usuario deberá crear en su PC. una carpeta denominada “Trabajo” desde la cual administrará y desarrollará las labores propias de su cargo, esta carpeta será en consecuencia la única objeto de backup por parte de la persona responsable de realizar backup en

Sistemas.
• En la Caja debe existir un sitio dedicado a guardar; backups, copias de los programas fuentes, ejecutables u objetos de los aplicativos más relevantes en la entidad, manuales, cd´s y licencias, esta debe existir en un edificio externo al sitio de operación diaria, este sitio se denominará cintoteca. Este sitio debe asegurar condiciones óptimas ambientales y de seguridad.
• El administrador de la red o persona a quien él designe, deberá respaldar en medios magnéticos la información de los servidores.
• El lugar de almacenamiento para las copias mensuales y anuales deberá ser el sitio externo que anteriormente fue denominado "cintoteca o hemeroteca". Este sitio debe asegurar condiciones óptimas ambientales y de seguridad.

1.4. AUTORIZACIONES

La autorización para el acceso de personal no autorizado al equipamiento de conectividad y a los servidores de datos debe ser gestionada ante la JGSC por la dependencia interviniente y deberá contar con la autorización expresa de la misma. Después que la autorización es otorgada, Sistemas pondrá los recursos a disposición del usuario, los usuarios no pueden acceder a ningún recurso informático de los mencionados hasta que les sea autorizado propiamente. No se permite la utilización de ningún usuario anónimo a menos que sea especificado, la autorización de acceso a los recursos es exclusiva al usuario al que le fue asignada y no es transferible a otros usuarios o dispositivos.

Los usuarios son responsables de entender y seguir los procedimientos administrativos establecidos para la utilización y el mantenimiento de los recursos informáticos de la Caja. Así mismo, son responsables de informarse y seguir las directivas administrativas comunicadas por correo u otros medios de información implementados o a implementarse.

Cada usuario es responsable del cuidado del hardware y software suministrado por la entidad. En consecuencia cada usuario responderá solidariamente por los daños y perjuicios técnicos o legales ocasionados por su mala utilización (La detección de este uso indebido podrá ocasionar la inhabilitación temporal o definitiva del sistema para el usuario responsable).

La Jefatura del Grupo de Sistemas de Comfaboy, es la dependencia responsable de coordinar la reparación de los equipos de cómputo de propiedad de la Caja. Las reparaciones o ampliaciones de los equipos no pueden ser hechas o contratadas por el usuario.

Identificaciones de usuarios.

Todos los usuarios que acceden a los recursos informáticos de la Caja, requieren de una única e intransferible identidad, normalmente un username, y un nombre de máquina para un dispositivo. Esta identidad se usa para representar un usuario o dispositivo en los ambientes informáticos de la red. Sistemas proporcionará este identificador como parte del proceso de autorización. Los identificadores concedidos expiran automáticamente o, cuando la dependencia interviniente solicita expresamente a Sistemas las cesaciones de acceso para dicho identificador de usuario, o cuando se compruebe un uso indebido.

La desconexión de un dispositivo de su puerto autorizado y conexión a otro puerto de la red es una violación de esta política. Los computadores portátiles deben ser autorizados para usar cualquier puerto de la red. El mal uso de la identidad de un usuario o un dispositivo constituye falsificación o falsedad. Las acciones que involucren accesos desautorizados, impropios o el mal uso de recursos informáticos de la red están sujeto a sanciones disciplinarias.

Las Contraseñas

Los usuarios tienen la responsabilidad de resguardar el acceso a los recursos informáticos de la Caja mediante la utilización de contraseñas confidenciales, personales e intransferibles que les fueron confiadas. Estas contraseñas deben construirse de manera que sean difíciles de suponer o adivinar por otros usuarios preferiblemente alfanuméricos, deben expirar periódicamente y poseer una longitud mínima. Todas las acciones realizadas bajo los auspicios de un identificador de usuario y sus consecuencias legales son responsabilidad del usuario titular del identificador. Toda sospecha de vulnerabilidad en la seguridad debe ser notificada inmediatamente a Sistemas.

2. POLITICAS SISTEMAS DE INFORMACIÓN

2.1. REQUERIMIENTO DE DESARROLLOS DE APLICACIONES

El desarrollo de nuevos sistemas de información será iniciado por pedido de los responsables de los procesos, realizando una solicitud a la JGSC, quien considerará el pedido y su impacto, establecerá su aprobación o no, y fijara la prioridad de ejecución, en función de factores como oportunidad, impacto en la gestión y costo. El desarrollo y cambios en un aplicativo es responsabilidad del área de desarrollo en sistemas, ya sean con recursos propios o servicios adquiridos por terceras personas, debiéndose ajustar a la metodología de desarrollo descrita en este documento.

METODOLOGÍA DE DESARROLLO DE SISTEMAS DE INFORMACIÓN

La JGSC define e implementa para el desarrollo y mantenimiento de sus sistemas de información una metodología de desarrollo que comprenda todas las fases en el ciclo de vida de productos de software como son:

• Alcance. Establecimiento de los objetivos y las fronteras del proyecto, conocimiento de los problemas y las necesidades del usuario, realizar reuniones con el usuario para determinar los acuerdos de responsabilidades.
• Planeación. Objetivos y metas claramente definidos por etapas, lista de actividades a realizar con descripción de productos a generar, determinación de estimativos y de riesgos, beneficios, recursos requeridos, costos, consideraciones de tiempo, seguimiento con informes del progreso. Periódicamente se debe realizar revalidación del aplicativo.
• Diseño. Análisis de alternativas, herramientas de apoyo, producto, revisión de manuales, seguimiento al avance, planear la etapa de desarrollo, realizar revisiones con la dependencia solicitante, preparar el modelo, diseñar los procedimientos, diseñar controles, preparar manual de usuarios
• Desarrollo. Revisar documentación generada en etapas anteriores, asegurar que se completen los productos de la etapa, realizar seguimiento al avance y preparar informes periódicos, planear etapa de puesta en marca, realizar revisiones, instalar hardware y software, desarrollar o modificar el software, desarrollar el código.
• Prueba. Realizar pruebas unitarias, realizar pruebas de integración, probar las interfaces, hacer pruebas de recuperación y desempeño, probar controles y seguridad, verificar la transportabilidad y la facilidad de mantenimiento.
• Implementación o Puesta en Marcha. Asegurar que se entreguen los productos, evaluar resultados de desarrollo de desempeño y de aplicación, revisar mejoras o deficiencias potenciales, determinar si es necesario planear una revaluación de algún uso, pasar cada uso

de la aplicación a producción, instalar el uso de la aplicación, iniciar las bases de datos y las tablas, ajustar la aplicación, entregar la aplicación, discontinuar la aplicación anterior o algún uso.
• Mantenimiento. Se debe establecer una clara asignación de responsabilidades de soporte para mantener la aplicación operando efectiva y eficientemente para los usuarios, debe realizar soporte al aplicativo y a los usuarios.

Una metodología para el diseño y desarrollo de sistemas es necesaria para estandarizar la forma en que se desarrollan los proyectos de sistemas, el objetivo de contar con una metodología incluye:

• Reducir tiempo y costo requerido para el desarrollo, mantenimiento y operación.
• Estandarización de herramientas y lenguajes de desarrollo que permitan facilitar el entrenamiento del personal, agilizando la comunicación entre los usuarios, especialistas de sistemas, proveedores y consultores externos.
• Facilitar la migración a ambientes de hardware y software de base diferentes.

La metodología elegida, basada en el ciclo de vida de desarrollo de sistemas deberá será la apropiada para los sistemas a ser desarrolladas, adquiridas, implementadas y mantenidas. La metodología deberá asegurar que la documentación creada durante el desarrollo del sistema o de los proyectos de modificación coincida con estos estándares. Esta metodología debe ser revisada periódicamente, para asegurar que incluya técnicas y procedimientos actuales generalmente aceptados.

Estándares de desarrollo de aplicaciones. El área de desarrollo de sistemas de información usará herramientas integradas de análisis para capturar y mantener documentación relacionada con las fases de alcance, planeamiento y diseño de sistemas, con el objetivo de proveer un archivo computarizado de los requerimientos y diseños de aplicaciones de negocio que conduzcan a sistemas de información, reducir el tiempo y costos de desarrollo.

Acuerdo de responsabilidades. Durante la etapa de Alcance, se debe desarrollar y documentar una división apropiada de responsabilidades entre la JGSC y el área que solicita el desarrollo. Este acuerdo convierte los principios, roles y responsabilidades en una estructura específica para servir las necesidades del proyecto. Este acuerdo debe cubrir: Participantes, asignación de responsabilidades y actividades, procedimientos para manejo de cambios y solución de problemas, procedimientos a seguir para la planeación, seguimiento y la ejecución del trabajo, responsabilidades de otras áreas, responsabilidades para las pruebas y documentación de soluciones.

Modularidad. Las aplicaciones se desarrollaran en forma modular de manera tal que las interfaces con el usuario, la lógica de la aplicación y los datos sean funcionalmente independientes. Los módulos que componen la aplicación, incluyendo las definiciones de los datos, deberán ser rehusados con mínimas modificaciones. El objetivo de esta política es facilitar el desarrollo de nuevas aplicaciones, asegurar que las reglas sean implementadas uniformemente, permitiendo un crecimiento ordenado y eficiente.

Interface común con el usuario. Los sistemas desarrollados y que no atiendan necesidades técnicas específicas, deberán basarse en interfaces comunes para los usuarios, siendo el objetivo principal de esta política la reducción del tiempo de capacitación de los usuarios, facilitando el uso de las aplicaciones.

Documentación en línea. Es objetivo prioritario de la JGSC contar con toda la documentación y textos de ayuda en línea, de manera tal que sean accesibles desde los puestos de trabajo de los usuarios. Cuando sea técnicamente factible, el texto de ayuda será accesible por pantalla y estará asociado a la función ejecutada.

La documentación incluye todo el texto de ayuda para el usuario final del sistema y el encargado del mantenimiento y operación del sistema, de allí la importancia de que, en el evento que se esté desarrollando con bases de datos se debe entregar documentado, el modelo entidad relación y el diccionario de datos, en todos los aplicativos desarrollados o adquiridos por terceros se debe entregar documentación de usuario final. El cumplimiento de esta política es lograr que la documentación sea accesible en forma fácil e inmediata, incrementando la probabilidad de que la documentación este actualizada.

Entorno de pruebas. El área de desarrollo de sistemas de información establecerá un entorno de pruebas en el cual se probaran todos los cambios a las aplicaciones antes de ser puestas en producción. En esta fase es indispensable contar con la participación de un trabajador del área de Auditoría Interna. Este entorno de pruebas debe ser independiente de los datos y aplicaciones en producción para evitar interferencias con las mismas. Dependiendo de las características de la aplicación, el entorno de pruebas puede ser un sistema de computación dedicado, o una partición o región protegida. El objetivo de implementación de esta política es proteger los datos y aplicaciones en producción, como así proveer un entorno adecuado para las pruebas de integración de sistemas.

Migración de desarrollo a producción. El área de desarrollo de Sistemas deberá asegurar que la administración de cambios, así como el control y la distribución de software sean integrados apropiadamente en un sistema completo de administración de cambios. El proceso de control de cambios se completara de acuerdo a los procedimientos establecidos para el área de desarrollo de sistemas de información y no se implementaran cambios a las aplicaciones en producción a menos que hayan sido primero probadas en un entorno de pruebas, aprobadas por el responsable usuario de los aplicativos, solicitante del requerimiento de cambio.

El patrocinador del cambio será responsable por la coordinación de actividades para el traspaso de información a producción, incluyendo la capacitación de los usuarios. El objetivo principal de esta política es establecer procesos de control de calidad a fin de evitar la migración a producción de aplicaciones potencialmente erróneas.

Control de cambios. El área de desarrollo, propondrá los procedimientos y los controles para revisar los cambios propuestos a las aplicaciones críticas, sistemas de computación, software e equipamiento de comunicaciones y seleccionará la alternativa más adecuada, a través de una función que preparará la agenda de los cambios propuestos. El objetivo principal de esta política será confirmar que no haya impactos imprevistos en los procesos, usuarios, operaciones de sistemas de computación, comunicaciones, integridad de los datos, seguridad o tecnología.

Control y mantenimiento de versiones. Cada versión de software que entre en producción será almacenada en un archivo permanente y un medio magnético, del cual podrá ser recuperado para futuras auditorias o con propósitos de restauración. Cada versión de software tendrá un único identificador que permita asegurar que la versión en uso sea la correcta y acceder fácilmente a versiones previas de software. Herramientas automatizadas o manuales, serán usadas para registrar y controlar cambios realizados a las aplicaciones. Deberá registrarse la razón para cada cambio y el nombre de la persona responsable del requerimiento.

Distribución de software y datos. Versiones de software y datos que hayan sido adecuadamente probadas, y estén en condiciones de ser distribuidas a los servidores, computadoras personales, servidores de las redes locales y otras plataformas, deberán ser archivadas en bibliotecas apropiadamente controladas. Una vez que se encuentren en dichas bibliotecas, las versiones serán distribuidas utilizando

procesos sistemáticos que identificarán las plataformas de destino apropiadas. La distribución puede ser realizada a través de la red de comunicaciones, o soportes adecuados.

El objetivo principal de esta política es mantener un control estricto y poder auditar sobre todos los componentes de software usados y cumplir con los requerimientos de licencias para software comercialmente provisto. Esta política se aplica tanto para aplicaciones desarrolladas internamente, como para paquetes pre-programados. El procedimiento deberá mantener registros legibles por computadora que indiquen, para cada plataforma, el software y los datos que fueron distribuidos.

POLITICAS INFRAESTRUCTURA TECNOLÓGICA

La administración de recursos informáticos de la Caja es responsabilidad de la JGSC. Las funciones de administración incluyen la administración de los servidores de internet, bases de datos, supervisión del tráfico de la red, seguridad de accesos a la red y servicios como dominios, firewalls, proxys o la instalación de nuevos enlaces, hardware de conectividad tales como switch, hubs, routers, sniffers, o analizadores de protocolos, se utiliza la conexión de protocolos TCP/IP para permitir la conectividad de la red al servicio de Internet. Se prohíbe la utilización de protocolos alternativos de red sin la autorización expresa de Sistemas; la presencia de tal software o hardware no autorizado en la red es una seria violación de esta política.

Sistemas puede quitar de la red y confiscar sin advertencia cualquier dispositivo sospechoso de violación de esta política. Ninguna dependencia podrá instalar nuevos enlaces a internet, de ningún tipo, sin el consentimiento y supervisión previa, a fin de no alterar o interferir con dispositivos ya instalados propios de la Caja o ajenos a ella. Será responsabilidad de la JGSC el orientar, coordinar y proponer lineamientos para el website bajo el dominio de la Caja.

Website. El website es el sitio oficial de la Caja, ninguna página de áreas/dependencias/instituciones que guarden relación de dependencia institucional con ésta podrá ser considerada con el título de "página oficial" si está en otro dominio electrónico que sea distinto a comfaboy.com.co tampoco se podrá usar bajo el "nombre o logo de la Caja" fuera de este ámbito, o de aquellos que la entidad determine oficialmente, el medio para actualizar las páginas web de la Caja es vía SFTP.
Organización del Equipo de Trabajo del Grupo de Sistemas de Comfaboy. Está en cabeza del Proceso de Gestión Tecnológica definir la organización de las diferentes áreas de trabajo que van a integrarla, de acuerdo a niveles de complejidad y consecuentemente con las descripciones, misiones y responsabilidades de los puestos de trabajo. La razón principal para la administración centralizada de este equipo de trabajo es mantener la consistencia de las habilidades requeridas y las compensaciones para todos los integrantes de Sistemas, a fin de prestar asistencia en la evaluación, reclutamiento, capacitación y rotación de los mismos.

Capacitación del personal de Sistemas. La JGSC, es la responsable por la capacitación del personal integrante de la misma, de acuerdo a planes de capacitación elaborados por Sistemas, asegurando que todo el personal esté capacitado en el uso de la metodología, técnicas, tecnologías y estándares establecidos, permitiendo difundir rápida y coherentemente los conocimientos relacionados a la información y sus tecnologías asociadas.

Capacitación al usuario final. Sistemas proveerá capacitación consistente a los usuarios finales, con el objetivo de alcanzar la eficiencia en el uso de las tecnologías, haciendo la precisión que es responsabilidad de Gestión Humana coordinar todo lo concerniente a capacitación de los empleados.

Adquisición de bienes de informática y sistemas. La adquisición de bienes de informática y de Sistemas en la Caja, quedará sujeta a los lineamientos establecidos en este documento. Toda adquisición de tecnología informática y de sistemas que se haga en la Caja deberá contar con el concepto técnico de la Jefatura del Grupo de Sistemas de Comfaboy (“JGSC”). La Caja, al planear las operaciones relativas a la adquisición de bienes informáticos y de sistemas (software-hardware), establecerá prioridades y en su selección tomará en cuenta: estudio técnico, precio, calidad, experiencia, desarrollo tecnológico, estándares y capacidad, entendiéndose por:

• Precio. Adquisición inicial del bien, accesorios y mantenimiento preventivo y correctivo.
• Calidad. Parámetro cualitativo que especifica las características técnicas de la tecnología de información.
• Experiencia. Presencia en el mercado nacional e internacional, estructura de servicio, la confiabilidad de los bienes y certificados de calidad con los que se cuente.
• Desarrollo Tecnológico. Se deberá analizar su grado de obsolescencia, nivel tecnológico con respecto a la oferta existente y su permanencia en el mercado.
• Estándares. Toda adquisición se basará en estándares que para tal fin establecerá periódicamente la JGSC.
• Capacidades. Analizar si el producto satisface la demanda actual con un margen de holgura y si tiene capacidad de crecimiento para soportar la carga de trabajo del área donde será implementado.

Adquisición de Hardware. Los equipos que se adquieran, deberán estar dentro de las listas de ventas vigentes de los fabricantes o distribuidores y dentro de los estándares de la Caja, deberán tener tres (3) años de garantía en sitio como mínimo, deberán ser equipos integrados de fábrica, la marca de los equipos o componentes deberá contar con presencia y permanencia demostrada en el mercado nacional e internacional, así como con asistencia técnica local.
Los equipos Pcs, servidores, portátiles, impresoras, scanner integrados, plotter, cámaras web, etc., deberán apegarse a los estándares de Hardware y Software vigentes en el mercado y en la Caja, corroborando que los suministros (cintas, papel, toner, cartuchos etc.) se consigan fácilmente en el mercado y no estén sujetas a un solo proveedor. Conjuntamente con los equipos principales y sus accesorios, se deberán adquirir los accesorios necesarios para su correcto funcionamiento, de acuerdo con las especificaciones de los fabricantes, y esta adquisición debe manifestarse en el costo del presupuesto inicial. Los equipos complementarios deberán tener una garantía mínima de un año y deberán contar con el servicio técnico correspondiente.

Los equipos adquiridos deben contar, con asistencia técnica por parte del proveedor durante la instalación de los mismos. En cuanto se refiere a los computadores personales y los denominados servidores, equipos de comunicaciones como enrutadores y concentradores, y otros que se justifiquen por ser de operación crítica o de alto costo; al vencer su período de garantía, deben contar con un programa de mantenimiento preventivo y correctivo que incluya el suministro de refacciones. En la adquisición de equipos, se deberá incluir el software estándar vigente con su correspondiente licenciamiento, para el efecto se tendrán en cuenta los lineamientos para la adquisición de software que se enuncia en este documento.

Adquisición de Software. Para la adquisición de software estándar, la JGSC dará a conocer periódicamente las tendencias en tecnología de punta vigente, cuando una dependencia se encuentre interesada en adquirir cualquier software administrativo, utilitario o de gestión, debe solicitar mediante memorando concepto técnico a la JGSC.

En la generalidad de los casos, sólo se adquirirán las últimas versiones liberadas de los productos seleccionados, salvo situaciones específicas que se deberán justificar ante la JGSC. Todos los productos de software que se adquieran deberán contar con

licenciamiento, medios de uso, documentación técnica y operativa.

Instalación. La instalación de los equipos de cómputo, se tendrán en cuenta las recomendaciones respecto a ubicación que realice Gestión Humana – Grupo Salud Ocupacional. Además queda sujeta a los siguientes lineamientos:

• Los equipos de la entidad se instalarán en lugares adecuados, lejos de polvo y tráfico de personas, garantizando las condiciones para su adecuado funcionamiento.
• En áreas de atención al público, los equipos se instalarán de manera que éste no tenga acceso al equipo, salvo en aquellas situaciones en que sean dispuestos específicamente para consulta directa del público.
• Todas las áreas o dependencias administrativas y operativas deberán contar con un croquis actualizado de las instalaciones eléctricas y de comunicaciones de los equipos de cómputo en red (planos del cableado estructurado) los cuales deben estar resumidos y disponibles en su respectivo cuarto de equipos o comunicaciones.
• Las instalaciones eléctricas y de comunicaciones, deberán cumplir con los estándares vigentes y resguardadas del paso de personas o máquinas, y libres de cualquier interferencia eléctrica o magnética.
• En ningún caso, se permitirán instalaciones improvisadas o sobrecargadas.
• Los usuarios no podrán conectar a las tomas de corriente regulada identificadas actualmente de color naranja, ningún elemento diferente a los equipos de cómputo. Las instalaciones eléctricas que alimenten elevadores, aspiradoras, cafeteras, motores y otros equipos, deberán tener un circuito independiente según los estándares que rigen la materia.

Usos prohibidos: En el entendido que el presente documento de políticas es solo un marco de referencia para los usuarios y en virtud de la imposibilidad de enumerar toda prohibición existente, dejamos aquí constancia de que todo aquello que no se encuentra expresamente permitido se encuentra prohibido. A continuación se detalla una lista de usos de recursos informáticos prohibidos:

• Utilización de cualquier recurso informático de la Caja para propósitos comerciales o para ganancia personal.
• Utilización de cualquier recurso informático de la Caja de manera que viole cualquier norma vigente.
• Utilización de cualquier recurso informático de la Red para guardar o transportar material ilegal, pornográfico, que haga apología del crimen o violencia, ofensivo, lesivo al buen nombre y honor de otros, propagandas comerciales, cadenas, difusión de actividades lucrativas en general, o su utilización en actividades no relacionadas con las funciones propias del cargo.
• Instalación de hardware o software sin la autorización apropiada de la JGSC.
• Permitir a personal externo acceder a la tecnología de información de la Red sin la autorización de la “JGSC”. o jefe inmediato.
• Privar o intentar privar a otros usuarios de la utilización o acceso a recursos informáticos de la Red.
• Intentar penetrar la seguridad de cualquier comunicación de la red de computadoras o sistema de las computadoras.
• Utilización de identificadores (Nombre y Password) de usuarios ajenos.
• Crear, utilizar o distribuir los programas que puedan dañar los datos, archivos, aplicaciones, funcionamientos del sistema, o funcionamientos de la red.
• Capturar/desencriptar contraseñas o protocolos de comunicaciones.
• Inspeccionar, modificar, o copiar programas o datos sin la autorización de su dueño o que atente contra las leyes vigentes de legalidad del software o propiedad intelectual.
• Utilizar cualquier correo electrónico o sistema de mensajería, ajenos a la Red o no, para enviar contenido abusivo, ofensivo, obsceno, o saturar los canales de comunicaciones, o el envío "cadenas de cartas", y otros esquemas que pueden causar tráfico excesivo en la red o cargar los sistemas informáticos.
• Alterar el software o la configuración del hardware de cualquier computadora o agregar cualquier dispositivo o sistema a la red sin el permiso de la JGSC.
• Utilizar Software comercial ilegalmente copiado o de libre distribución que no esté incluido en los estándares, o que no esté involucrado con el objeto laboral de la dependencia. En caso de necesitar de la instalación de algún software adicional se deberá contar con la autorización de la “JGSC”, de lo contrario se deberá utilizar el predeterminado del equipo de cómputo.
• Utilización de la red para ganar o intentar ganar el acceso desautorizado a los recursos de información locales o remotos.
• Utilización de cualquier software o hardware que pueda comprometer la seguridad de la red o de cualquier recurso informático de la misma.
• Revelar claves o código de usuario, base de datos, aplicativos, o código para llamadas.
• Usar la información de Comfaboy para actividades ajenas de la entidad.
• Ingresar a una cuenta o aplicación para la cual usted no está autorizado.
• Falsificar información de configuración de enrutamiento y de configuración de equipos y sistemas con el objetivo de provechar alguna vulnerabilidad.
• Burlar los mecanismos de seguridad de cualquier servicio de red, aplicativo, servidor o cuenta de usuario.

El inadecuado uso de los recursos informáticos podrá dar lugar al inicio de actuaciones disciplinarias respecto a cualquier usuario de los servicios.

REDES Y COMUNICACIONES

Este servicio se brindará a través de una única red que interconectará todos los servidores y equipos de cómputo de las diferentes dependencias de la Caja, para facilitar el acceso a las aplicaciones y datos, asegurando la consistencia e integridad de la misma, evitando la duplicación de información, y minimizando costos.

El servicio de comunicaciones y la topología de la red no deben afectar la seguridad y el acceso a las aplicaciones y a los datos de las dependencias, debiendo en cualquiera de los casos permitir el control y la administración de las aplicaciones y datos independientemente de la ubicación física de los mismos.

Administración de la red.

Los tres principios básicos que deben cumplir las redes son: Confidencialidad: Deberá garantizar la protección adecuada de los datos para evitar que algún intruso pueda obtener información de la entidad. Disponibilidad: La red deberá estar disponible en todo momento, manteniendo una velocidad de respuesta adecuada, e Integridad: La red debe mantener información tal y como ha sido almacenada desde un principio, sin información incoherente. Dentro de los procesos incluye el monitoreo del tráfico y del rendimiento de cada componente de la red. Estas funciones y responsabilidades estarán centralizadas, siendo la JGSC quien defina en que trabajador recae la responsabilidad.

Con propósitos de auditoría, resolución de problemas técnicos o investigar violaciones a las políticas institucionales de la Caja, el Jefe de Sistemas podrá autorizar a sus Trabajadores a inspeccionar todos los dispositivos informáticos que se encuentren o no conectados a la red, toda vez que sea necesario y sin previo trámite.

Cuando sea factible y recomendable por la minimización de los costos e incremento de la eficiencia, se contratara a proveedores externos para instalación, mantenimiento de la red de comunicaciones de voz y datos. Sistemas, seleccionará los protocolos a ser usados requiriendo servicios del más alto nivel a fin de proveer la conectividad necesaria para el transporte de archivos, acceso a bases de datos y otros servicios.

Conectividad. La Tecnología tiene la capacidad para abrir las puertas a un vasto mundo de recursos de información, con una conexión a Internet. Las oportunidades que tenemos con esta conectividad son casi ilimitadas, mas no así, los recursos computacionales y de conectividad disponibles. Este nuevo mundo virtual al que tenemos acceso requiere de reglas y precauciones, para asegurar un uso óptimo y correcto de los recursos. En este sentido, la JGSC cree firmemente en que el desarrollo de políticas que sean bien entendidas, que circulen ampliamente y que sean efectivamente implementadas, conllevará a hacer de la Red de la Caja y el Internet un ambiente seguro y productivo para Trabajadores y miembros en general de la comunidad.

Se trata entonces de presentar lo que se conoce como Políticas y Reglamentos para el Uso Aceptable para los recursos computacionales y de conectividad presentes en la red. Estas políticas establecen entre otras cosas, el comportamiento esperado hacia diferentes servicios de información y las reglas en cuanto al uso adecuado de recursos físicos.

Términos / Definiciones.

• Red: Conjunto de recursos de conectividad y computacionales que permite la comunicación de datos e información a través de todas las dependencias e Internet.
• Domain Name Server: Servidores que mantienen diferente tipo de información como bases de datos, correo electrónico, página web y información acerca de las computadoras e Internet.
• Dirección IP: un número único que identifica una computadora en Internet. Por ejemplo 17.16.160.1
• Estación segura: Computadora que cumpla con los requerimientos mínimos de seguridad de comunicación de datos estipulados por el grupo de Servicios de Redes.
• Username: Nombre con que se identifica la cuenta de un usuario en un servidor.
• Password: Clave secreta de identificación por cada uno de los usuarios en un serivdor
• Root: Usuario de un sistema con mayores privilegios administrativos.

Políticas

• La función de la red de Comunicaciones e información es "transportar" datos que soporten el flujo de la información de la entidad
• El uso de la red por individuos u organizaciones que no sean parte de los Trabajadores de la Caja, no está permitido, si exista alguna información que deba ser consultada por un ciudadano este debe estar apoyado por un trabajador de la Caja.
• El acceso a Internet debe hacerse desde una estación debidamente registrada y/o autorizada por el grupo de Redes y Comunicaciones. Dicho de otra forma, el computador debe estar registrado dentro del DNS (Domain Name Server) primario de la Caja y estar localizado con una dirección IP legítima. La estación debe soportar e implementar protección de clave de usuario y sistemas de seguridad de redes actualizados.
• Las políticas de uso aceptable de la red incluyen el uso de la red de comunicación para el propósito, Misión y Visión de la Caja de soportar diferentes actividades que busquen cubrir los objetivos fundamentales de la entidad.
• El uso de la red de comunicaciones para ganancias y actividades financieras no relacionadas con las actividades normales de la entidad es catalogado como una práctica inaceptable.
• Debido a que la JGSC se esforzará en mantener la privacidad de las comunicaciones personales y un nivel de servicio apropiado, la infraestructura tecnológica monitoreará la carga de tráfico de la red y cuando sea necesario tomará acción para proteger la integridad y operatividad de sus redes.

Servicios de la red.

La autorización para conectar dispositivos adicionales a la red o adicionar servicios a la red debe obtenerse por la JGSC, no pueden conectarse computadoras, servidores, hubs, switches, routers, access point, o cualquier otro hardware a la red sin la debida autorización. Sistemas puede quitar de la red y confiscar sin advertencia cualquier dispositivo sospechado de violación a esta política.

En caso de que se obtenga la autorización apropiada, Sistemas permitirá a una computadora personal la conexión a la red. Esta autorización sólo es para la computadora y para ser usada como un cliente normal en la red y no proporcionar ningún servicio a la red. El uso de las computadoras como gateways o routers a otra red o como servidor de acceso remoto por módem está prohibido sin la autorización expresa de Sistemas. La JGSC podrá:

• Recolectará estadísticas de utilización basado en las direcciones de redes, protocolo de red, y tipo de aplicación.
• Progresivamente restringirá usuarios, cuando su utilización de la red resulte en la degradación del rendimiento. Tal restricción será notificada a los usuarios a través de medios apropiados.
• Las facilidades de redes no pueden ser usadas por cualquier individuo o grupos de personas para cualquier actividad de naturaleza ilegal o fraudulenta, incluyendo actividades ilegales como las definidas por las leyes, así como políticas, códigos y regulaciones de la Caja
• Cualquier actividad que se sospeche ilegal o fraudulenta debe ser inmediatamente reportada a la autoridad competente.
• A los usuarios que quebranten estas políticas y reglamentos de uso y acceso, les será eliminado el acceso a las redes de comunicación y computadoras de la Caja. Todos los otros estándares de conducta aplican al uso de la red y sus recursos.

Cableado Estructurado. Tiene como objetivo dar flexibilidad a las instalaciones permitiendo la conexión de equipos capaces de transmitir voz y datos. Es indispensable y recomendable que todo el sistema de cableado estructurado se comporte como un canal o sea que desde el cable de estación hasta el Patch Cord, sean de la misma marca que el fabricante asegure que no existan cambios de impedancia en ningún punto, lo cual garantiza que la atenuación por este motivo sea nula y esto redundará en un mejor rendimiento de la red.

La ventilación y climatización debe ser para temperaturas ambientes promedias, inferiores o iguales a 28º centígrados, los cuartos de cableados en la Caja, deben contar con dos entradas de ventilación provistas de rejilla, una de ellas en la zona inferior del cuarto y otra en la zona superior. Es recomendable instalar un extractor de aire en la apertura superior y un filtro de aire en la apertura inferior, este filtro puede ser de tipo aire acondicionado.

Es deseable e indispensable que todos los cuartos de equipo tengan alimentación de corriente ininterrumpida (UPS) de tipo On-line con

capacidad de alimentar todos los equipos que se conectarán al centro de cableado, con el fin de mantener los servicios de red aún en casos de falla del fluido eléctrico.

Firewalls. Es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada o pública y el Internet. El firewall determina cuál de los servicios de red puede ser acezado dentro de ésta por los que están fuera, es decir, quien puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo tráfico de información a través del Internet deberá pasar a través de él mismo donde podrá ser inspeccionada la información. Un firewall debe contar con sistemas de detección de intrusos. El firewall podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración, desafortunadamente, este sistema no pude ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este. Un firewall es vulnerable, él no protege de la gente que está dentro de la red interna, éste trabaja mejor si se complementa con una defensa interna.

Correo Electrónico. La Jefatura de Sistemas de Comfaboy, promoverá el uso del correo electrónico, como medio de comunicación institucional, monitoreará periódicamente o por solicitud de los organismos de control, los registros de entrada y salida de los e-mail y los accesos a Internet para verificar la adecuada utilización de este recurso. El uso de Internet, deberá ser estrictamente de carácter institucional de acuerdo a las políticas internas que se establezca para su utilización.

El uso del correo estará sujeto a las disposiciones nacionales e internacionales vigentes. Todas las dependencias que guarden relación deberán poseer una cuenta de correo electrónico, para incorporarse a las listas de correo pertinentes, a fin de facilitar la comunicación y conectividad institucional. La consulta de esta cuenta será de obligación diaria.

LISTA DE VERSIONES

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
2	05/Dic/2011	Se eliminó del capítulo 1.3- Respaldos la tabla 1.3.1 –Tabla frecuencia de BACKUP de datos, 1.3.2-Tabla frecuencia de restauración de datos, tabla 1.3.3 Tabla frecuencia de BACKUP de fuentes; al igual que la rotulación de las cintas. En el capítulo de políticas sistema de información- 2.2 metodología de desarrollo de sistemas de información- documentación en línea se eliminó “en papel”; también se eliminó la distribución de la documentación. Se adicionó en el capítulo 3-Políticas infraestructura tecnológica “swich”. Se eliminó del capítulo Políticas infraestructura tecnológica - el procedimiento de procesamiento. Dentro de los usos prohibidos “para propósitos comerciales”. Se incluye en los usos prohibidos: Revelar claves o código de usuario, base de datos, aplicativos, o código para llamadas, Usar la información de Comfaboy para actividades ajenas de la entidad, Ingresar a una cuenta o aplicación para la cual usted no está autorizado, Falsificar información de configuración de enrutamiento y de configuración de equipos y sistemas con el objetivo de provechar alguna vulnerabilidad, Burlar los mecanismos de seguridad de cualquier servicio de red, aplicativo, servidor o cuenta de usuario. Se elimina en el numeral 3.1.2 Servicios de la red “Seguridad de los módems de acceso telefónico”.
3	11/Dic/2018	Se modificaron todos los items
4	02/Dic/2020	Se actualiza todo el documento

ELABORÓ	REVISÓ	APROBÓ
Nombre: Lady Carolina Gonzalez Moreno **Cargo:** Contratista **Fecha:** 02/Dic/2020	**Nombre:** Orlando Rodriguez Castillo **Cargo:** Jefe Grupo Sistemas **Fecha:** 02/Dic/2020	**Nombre:** Jaime Fernando Diaz Molina **Cargo:** Jefe Departamento de Planeación e Informática **Fecha:** 03/Dic/2020