## 1. OBJETIVO

Establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, dispositivos, sistemas de información, redes (Voz y Datos)) y personas que interactúan haciendo uso de los servicios asociados a ellos y se aplican a todos los usuarios de cómputo de la empresa.

## 2. ALCANCE

Este procedimiento aplica para el conocimiento de las políticas de seguridad informática establecidas dentro de la institución y aplica a todos los empleados, contratistas, consultores, eventuales y otros empleados de la Empresa EMDUPAR S.A. E.S.P., incluyendo a todo el personal externo que cuenten con un equipo conectado a la red.

## 3. RESPONSABILIDAD Y AUTORIDAD

**El Jefe de la División de Sistemas de Información** es la autoridad para aplicar y hacer cumplir este procedimiento y junto con el personal del área de sistemas son los responsables de vigilar e implementar las políticas de seguridad informática establecidas, direccionados por el jefe del área.

## 4. DEFINICIONES

**4.1.** **Seguridad informática:** es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

**4.2.** **ABD:** Administrador de Base de Datos.

**4.3.** **Data Center:** (Centro de Datos) Oficina con equipos de cómputo, telecomunicaciones y servidores que prestan servicios a todas Las Empresas con las características físicas y ambientales adecuadas para que los equipos alojados funcionen sin problema.

**4.4. Contraseña:** Es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. (password). La contraseña debe mantenerse en secreto ante aquellos a quien no se le permite el acceso.

**4.5. Confidencial:** Significa que la información no esté disponible o revelada a individuos, entidades o procesos no autorizados.

**4.6. Correo Electrónico Institucional:** Es el servicio basado en el intercambio de información a través de la red y el cual es provisto por EMDUPAR S.A. E.S.P., para los funcionarios, autorizados para su acceso. El propósito principal es compartir información de forma rápida, sencilla y segura. El sistema de correo electrónico puede ser utilizado para el intercambio de información, administración de libreta de direcciones, manejo de contactos, administración de agenda y el envío y recepción de documentos, relacionados con las responsabilidades institucionales.

**4.7. Red:** Equipos de cómputo, sistemas de información y redes de telemática de las Empresas.

**4.8. Solución Antivirus:** Recurso informático empleado para solucionar problemas causados por virus informáticos.

**4.9. Disponibilidad de la información:** La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. La disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

**4.10. Estrategia de Gobierno en Línea**: Estrategia definida por el Gobierno Nacional que busca apoyar y homologar los contenidos y servicios ofrecidos por cada una de las entidades públicas para el cumplimiento de los objetivos de un Estado más eficiente, transparente y participativo, donde se presten servicios más eficientes a los ciudadanos a través del aprovechamiento de las tecnologías de información.

**4.11. Seguridad de la información:** Hace referencia a la preservación de la confidencialidad (propiedad de que la información, significa que no esté disponible o revelada a individuos no autorizados, entidades o procesos.), integridad (protección de la exactitud e integridad de los activos) y disponibilidad (propiedad de ser accesibles y utilizables a la demanda por una entidad autorizada) de la información.

**4.12. Servicio:** Es el conjunto de acciones o actividades de carácter misional diseñadas para incrementar la satisfacción del usuario, dándole valor agregado a las funciones de la entidad.

**4.13. Sistemas de Información:** Un 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 o un objetivo.

**4.14. Virus informático:** Programa ejecutable o pieza de código con habilidad de ejecutarse y reproducirse, regularmente escondido en documentos electrónicos, que causan problemas al ocupar espacio de almacenamiento, así como destrucción de datos y reducción del desempeño de un equipo de cómputo.

## 5. DESARROLLO

### 5.1. ACCESO A LA INFORMACION

Todos los funcionarios que laboran para EMDUPAR S.A. E.S.P. deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. En el caso de personas externas a EMDUPAR S.A. E.S.P., el jefe del área u Oficina responsable de generar la información debe autorizar sólo el acceso indispensable de acuerdo con el trabajo realizado por estas, previa justificación de la persona.

Para dar acceso a la información o al software de la empresa, el jefe inmediato del trabajador deberá enviar un correo a soporte@emdupar.gov.co indicando las opciones y accesos que se habilitaran, la cual deberá realizarse de acuerdo con la

importancia de la información en la operación normal de la Entidad. El otorgamiento de acceso a la información está regulado mediante las normas y procedimientos definidos para tal fin.

En el caso que se requiera el registro de eventos en los diversos componentes de la plataforma tecnológica se efectuará un seguimiento a los accesos realizados por los usuarios a la información de la Entidad, con el objeto de minimizar el riesgo de pérdida de integridad de la información. Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información se deberán documentar y realizar las acciones tendientes a su solución.

## 5.2. ADMINISTRACION DE CAMBIOS

Todo cambio a un componente de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.

Todo cambio que afecte la plataforma tecnológica debe ser requerido por los usuarios de la información y aprobado formalmente por el responsable de la administración del componente tecnológico, Jefe de Oficina, Líder de Proceso o a quienes estos formalmente deleguen.

Bajo ninguna circunstancia un cambio puede ser aprobado, realizado e implantado por otra persona o área diferente a la de la División de Sistemas de Información, encargada de la plataforma tecnológica.

Para la administración de cambios se efectuará el procedimiento correspondiente definido por EMDUPAR S.A. E.S.P., de acuerdo con el tipo de cambio solicitado en la plataforma tecnológica.

Cualquier tipo de cambio en la plataforma tecnológica debe quedar formalmente documentado desde su solicitud vía correo electrónico soporte@emdupar.gov.co hasta su implantación. Este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos.

## 5.3. ADMINISTRACION DE LA SEGURIDAD

La función de administración de la seguridad será realizada por los funcionarios de la División de Sistemas de Información y por los administradores de la seguridad informática para cada sistema aplicativo.

La División de Sistemas de Información se encargará de la definición y actualización de las políticas, normas, procedimientos y estándares relacionados con la seguridad informática, igualmente velará por la implantación y cumplimiento de las mismas.

Para realizar la función de administración de la seguridad los responsables se apoyarán en herramientas tecnológicas que permitan una adecuada administración, monitoreo y control de los recursos informáticos (Servidor de dominio, Antivirus, FortiGate, Contraseñas de acceso, niveles de acceso, entre otros).

## 5.4. ALMACENAMIENTO Y RESPALDO DE LA INFORMACIÓN

La información que es soportada por la infraestructura de tecnología informática de EMDUPAR S.A. E.S.P. deberá ser almacenada y respaldada de acuerdo con las normas emitidas de tal forma que se garantice su disponibilidad.

Debe existir una definición formal de la estrategia de generación, retención y rotación de las copias de respaldo. El almacenamiento de la información deberá realizarse interna y/o externamente a la Entidad, esto de acuerdo con la importancia de la información para la operación de EMDUPAR S.A. E.S.P.

El área dueña de la información en conjunto con la División de Sistemas de Información definirá la estrategia a seguir para el respaldo de la información.

## 5.5. SEGURIDAD INFORMATICA

La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí

contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Podemos entender como seguridad un estado de cualquier tipo de información (informático o no) que nos indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro.

**Para que un sistema se pueda definir como seguro debe tener estas cuatro características:**

- **Integridad:** La información sólo puede ser modificada por quien está autorizado y de manera controlada.
- **Confidencialidad:** La información sólo debe ser legible para los autorizados.
- **Disponibilidad:** Debe estar disponible cuando se necesita.
- **Irrefutabilidad** (No repudio): El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

Dependiendo de las fuentes de amenaza, la seguridad puede dividirse en seguridad física, seguridad ambiental y seguridad lógica.

En estos momentos la seguridad informática es un tema de dominio obligado por cualquier usuario de la Internet, para no permitir que su información sea comprometida.

**Estos fenómenos de riego pueden ser causados por:**

**El usuario:** causa del mayor problema ligado a la seguridad de un sistema informático (porque no le importa, no se da cuenta o a propósito).

**Programas maliciosos:** programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o maldad) en el ordenador abriendo una puerta a intrusos o bien modificando los datos. Estos

programas pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica o un programa espía o Spyware.

**Un intruso:** persona que consigue acceder a los datos o programas de los cuales no tiene acceso permitido (cracker, defacer, script kiddie o Script boy, viruxer, etc.).

**Un siniestro** (robo, incendio, por agua): una mala manipulación o una mal intención derivan a la pérdida del material o de los archivos.

**El personal interno de Sistemas.** Las pujas de poder que llevan a disociaciones entre los sectores y soluciones incompatibles para la seguridad informática.

**Tecnologías repelentes o protectoras:** cortafuegos, sistema de detección de intrusos, antivirus, llaves para protección de software, etc. Mantener los sistemas de información con las actualizaciones que más impacten en la seguridad.

**Consideraciones de software:** Tener instalado en la máquina únicamente el software necesario reduce riesgos. Así mismo tener controlado el software asegura la calidad de la procedencia del mismo (el software obtenido de forma ilegal o sin garantías aumenta los riesgos). En todo caso un inventario de software proporciona un método correcto de asegurar la reinstalación en caso de desastre. El software con métodos de instalación rápidos facilita también la reinstalación en caso de contingencia.

**Consideraciones de una red:** Los puntos de entrada en la red son generalmente el correo, las páginas web y la entrada de ficheros desde discos, o de ordenadores ajenos, como portátiles.

Mantener al máximo el número de recursos de red sólo en modo lectura, para impedir que ordenadores infectados propaguen virus. En el mismo sentido se pueden reducir los permisos de los usuarios al mínimo.

Controlar y monitorizar el acceso a Internet puede detectar, en fases de recuperación, cómo se ha introducido el virus.

## 5.6. LINEAMIENTOS DE LA DIVISIÓN DE SISTEMAS DE INFORMACIÓN

### 5.6.1. Lineamientos Generales

1. Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos para el desarrollo de sus actividades específicas.
2. Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).
3. Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.
4. Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.
5. Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.
6. Sensibilizar a los usuarios del sistema sobre los riesgos que amenazan la seguridad física del equipo.

### 5.6.2. Lineamientos Específicos

1. Para los administradores del sistema, no dejar el sistema, las unidades de cinta, las terminales o las estaciones de trabajo sin vigilancia durante largos períodos de tiempo. Conviene establecer algunas restricciones de acceso en los lugares donde se encuentren estos dispositivos.
2. No dejar la consola del sistema u otros dispositivos de terminal conectados como raíz y sin supervisión alguna.
3. Guardar las copias de seguridad en una zona segura y limite el acceso a dicha zona.

## 5.7. VIGENCIA

Todas las amenazas informáticas están en continuo proceso de expansión, lo que, unido al progresivo aumento de los sistemas de información y dependencia del negocio, hace que todos los sistemas y aplicaciones estén expuestos a riesgos cada vez mayores, que, sin una adecuada gestión de los mismos, pueden

ocasionar que su vulnerabilidad se incremente y consiguientemente los activos se vean afectados. Todo empleado es responsable del cumplimiento de los estándares, directrices y procedimientos de control de acceso, así como también notificar a su jefe inmediato, cuando por algún motivo no pueda cumplir con las Políticas de Seguridad indicando el motivo por el cual no le es posible apegarse a la normativa de seguridad.

Cabe destacar que este nivel de responsabilidad va a ser conocido por los diferentes jefes de áreas de EMDUPAR S.A. E.S.P., quienes serán los garantes de que esta información sea conocida por cada integrante de área. La documentación presentada como Políticas de Seguridad entrará en vigencia desde el momento en que sean aprobadas por la Gerencia. Esta normativa deberá ser revisada y actualizada conforme a las exigencias de EMDUPAR S.A. E.S.P. o en el momento en que haya la necesidad de realizar cambios sustanciales en la infraestructura tecnológica.

## 5.8. LICENCIAMIENTO

Todos los productos de Software que se utilicen dentro de EMDUPAR S.A. E.S.P. deberán contar con su factura y licencia de uso respectiva; por lo que se promoverá la regularización o eliminación de los productos que no cuenten con el debido licenciamiento.

## 5.9. BASES DE DATOS

Para la operación de los software y aplicaciones de red en caso de manejar los datos empresariales mediante sistemas de información, se deberá tener en consideración lo siguiente:

- Toda la información de EMDUPAR S.A. E.S.P. deberá invariablemente ser operada a través de un mismo tipo de sistema manejador de base de datos para beneficiarse de los mecanismos de integridad, seguridad y recuperación de información en caso de presentarse alguna falla.
- El acceso a los sistemas de información, deberá contar con los privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad total de

la información de EMDUPAR S.A. E.S.P. Los niveles de seguridad de acceso deberán controlarse por el ABD y poder ser manipulado por software.

- Se deben delimitar las responsabilidades en cuanto a quién está autorizado a consultar y/o modificar en cada caso la información, tomando las medidas de seguridad pertinentes.
- Los datos de los sistemas de información, deben ser respaldados de acuerdo a la frecuencia de actualización de sus datos, guardando respaldos históricos periódicamente. Es indispensable llevar una bitácora oficial de los respaldos realizados, así mismo, los CDs, DVDs, Blue Ray, cartuchos de respaldo, deberán guardarse en un lugar de acceso restringido con condiciones ambientales suficientes para garantizar su conservación. En cuanto a la información de los equipos de cómputo personales, se recomienda a los usuarios que realicen sus propios respaldos en los servidores de respaldo externo (Nube) o en medios de almacenamiento alternos (disco D, USB, Nube).
- Todos los sistemas de información que se tengan en operación, deben contar con sus respectivos manuales actualizados.
- Los sistemas de información, deben contemplar el registro histórico de las transacciones sobre datos relevantes, así como la clave del usuario y fecha en que se realizó (Normas Básicas de Auditoria y Control).
- Se deben implantar rutinas periódicas de auditoria a la integridad de los datos y de los programas de cómputo, para garantizar su confiabilidad.

## 5.10. FRECUENCIA DE EVALUACIÓN DE LAS POLÍTICAS

Se evaluarán las políticas del presente documento, con una frecuencia anual.

## 5.11. ACCESO FÍSICO

La Empresa destinará un área que servirá como centro de telecomunicaciones (Data Center) donde ubicarán los sistemas de telecomunicaciones y servidores. Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada de manera que el usuario no tenga acceso físico directo. Entendiendo por sistema de comunicaciones: el equipo activo y los medios de comunicación.

El acceso de terceras personas debe ser identificado plenamente, controlado y vigilado durante el acceso portando una identificación que les será asignado por el área de seguridad de acceso al edificio y a las oficinas de EMDUPAR S.A. E.S.P. Las visitas internas o externas podrán acceder a las áreas restringidas siempre y cuando se encuentren acompañadas cuando menos por un responsable de la División de Sistemas de Información o con permiso de estos. Las visitas a las instalaciones físicas de los centros de telecomunicaciones se harán en el horario establecido.

## 5.12. PROTECCIÓN FÍSICA

### 5.12.1. Data Center

El DataCenter deberá:

- Ser un área restringida. Tener un sistema de control de acceso que garantice la entrada solo al personal autorizado por el jefe de la División de Sistemas de Información.
- Recibir limpieza al menos una vez por semana, que permita mantenerse libre de polvo.
- Estar libre de contactos e instalaciones eléctricas en mal estado.
- Aire acondicionado. Mantener la temperatura a 21 grados centígrados, 24 horas del día, 365 días del año.
- Respaldo de energía redundante.
- Seguir los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores.
- Los sistemas de tierra física, sistemas de protección e instalaciones eléctricas deberán recibir mantenimiento anual con el fin de determinar la efectividad del sistema.
- Control de humedad.
- Prevención y/o detección de incendios
- Sistemas de extinción.
- Contar por lo menos con dos extintores de incendio adecuado y cercano al Data Center.

### 5.12.2. Infraestructura

Las dependencias deberán considerar los estándares vigentes de cableado estructurado durante el diseño de nuevas áreas o en el crecimiento de las áreas existentes. El resguardo de los equipos de cómputo deberá quedar bajo la División de Sistemas de Información contando con un control de los equipos que permita conocer siempre la ubicación física de los mismos.

## 5.13. INSTALACIONES DE EQUIPOS DE CÓMPUTO

La instalación del equipo de cómputo, quedará sujeta a los siguientes lineamientos:

- La instalación de los equipos de cómputo y dispositivos será realizada solo por el personal de la División de Sistemas de Información, con su previa solicitud enviada al correo soporte@emdupar.gov.co
- Los equipos para uso interno se instalarán en lugares adecuados, lejos de polvo y tráfico de personas.
- Las instalaciones eléctricas y de comunicaciones, estarán preferiblemente fijas o en su defecto resguardadas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.
- Las instalaciones se apegarán estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios.

## 5.14. CONTROL

- Los funcionarios de la División de Sistemas de Información deben llevar un control total y sistematizado de los recursos de cómputo y licenciamiento.
- El jefe de la División de Sistemas de Información es el responsable de organizar al personal auxiliar encargado del mantenimiento preventivo y correctivo de los equipos de cómputo de la empresa.
- El área de Gestión Humana de la empresa deberá reportar a la División de Sistemas de Información cuando un usuario ingrese o deje de laborar con la empresa con el fin de retirarle las Políticas de Seguridad Informática

credenciales de ingreso a los recursos y supervisar la correcta devolución de los equipos y recursos asignados al usuario.

## 5.15. RESPALDOS

- Las Bases de Datos de EMDUPAR S.A. E.S.P. serán respaldadas diaria y periódicamente en forma automática y manual, según los procedimientos generados para tal efecto.
- Las Bases de Datos deberán tener una réplica en uno o más equipos remotos alojados en un lugar seguro (Nube) que permita tener contingencia y continuidad.
- Los servidores de hosting estarán alojados en netfirms.com.
- Los demás respaldos (una copia completa) deberán ser almacenados en un lugar seguro y distante del sitio de trabajo, en bodegas con los estándares de calidad para almacenamiento de medios magnéticos.
- Para reforzar la seguridad de la información, los usuarios, bajo su criterio, deberán hacer respaldos de la información en sus discos duros (D, E, USB), dependiendo de la importancia y frecuencia de cambio; y en las unidades de almacenamiento asignadas por la Empresa en “La Nube”, deberá realizar una sincronización continua de la información importante de la empresa. Los respaldos serán responsabilidad absoluta de los funcionarios.

## 5.16. RECURSOS DE LOS FUNCIONARIOS

### 5.16.1 Uso

- Los funcionarios deberán cuidar, respetar y hacer un uso adecuado de los recursos de cómputo, impresoras y Red de EMDUPAR S.A. E.S.P, de acuerdo con las políticas que en este documento se mencionan.
- Los funcionarios deberán solicitar apoyo a la División de Sistemas de Información ante cualquier duda en el manejo de los recursos de cómputo de la Empresa.
- El correo electrónico no se deberá usar para envío masivo, materiales de uso no institucional o innecesarios (entiéndase por correo masivo todo aquel que

sea ajeno a la Empresa EMDUPAR S.A. E.S.P., tales como cadenas, publicidad y propaganda comercial, política, social, etcétera).

### 5.16.2 Derechos de Autor

- Queda estrictamente prohibido inspeccionar, copiar y almacenar programas de cómputo, software y demás fuentes que violen la ley de derechos de autor, para tal efecto todos los funcionarios quedan notificados con la socialización de este documento, donde se comprometan bajo su responsabilidad, a no usar programas de software que violen la ley de derechos de autor. Para asegurarse de no violar los derechos de autor, no está permitido a los funcionarios copiar ningún programa instalado en los computadores de la Empresa bajo ninguna circunstancia sin la autorización escrita de la Gerencia o del Jefe de la División de Sistemas. No está permitido instalar ningún programa en su computadora sin dicha autorización o la clara verificación de que la Empresa posee una licencia que cubre dicha instalación.
- No está autorizada la descarga de Internet, de programas informáticos no autorizados por la Gerencia o por el jefe de la División de Sistemas.
- No se tolerará que un empleado realice copias no autorizadas de programas informáticos.
- No se tolerará un empleado realice intercambios o descargas de archivos digitales de MP4, MP3, WAV, PELICULAS, JUEGOS, PORNOGRAFIA, entre otros, de los cuales no es el autor o bien no posee los derechos de distribución del mismo.
- El personal encargado del soporte de Tecnología revisará las computadoras constantemente para realizar un inventario de las instalaciones de programas informáticos y determinar si la Empresa posee licencias para cada una de las copias de los programas informáticos instalados.
- Si se encuentran copias sin licencias, estas serán eliminadas y, de ser necesario, reemplazadas por copias con licencia.
- Los funcionarios no descargarán ni cargarán programas informáticos no autorizados a través de Internet.
- Los funcionarios que se enteren de cualquier uso inadecuado que se haga en la Empresa EMDUPAR S.A. E.S.P. de los programas informáticos o la

documentación vinculada a estos, deberán notificar al Gerente o el jefe de la División de Sistemas.

- Los empleados que realicen, adquieran o utilicen copias no autorizadas de programas informáticos estarán sujetos a sanciones disciplinarias internas de acuerdo a las circunstancias.

## 5.17. CORREO ELECTRONICO

- La División de Sistemas de Información se encargará de asignar las cuentas a los funcionarios para el uso de correo electrónico en los servidores que administra.
- Para efecto de asignarle su cuenta de correo al funcionario, el área de Recursos Humanos o el jefe inmediato deberá enviar un correo a soporte@emdupar.gov.co, especificando el nombre, cedula y cargo del funcionario para el cual se necesita de la creación del correo.
- La cuenta será activada en el momento en que el funcionario ingrese por primera vez a su correo y será obligatorio el cambio de la contraseña de acceso inicialmente asignada.
- La Contraseña debe llevar una combinación de caracteres alfabéticos, numéricos y con letra mayúscula al inicio con una longitud mínima de ocho dígitos.

## 5.18. BASES DE DATOS Y SOFTWARE.

- El Administrador de la Base de Datos no deberá eliminar ninguna información del sistema, a menos que la información esté dañada o ponga en peligro el buen funcionamiento del mismo.
- El Administrador de la Base de Datos es el encargado de asignar las cuentas a los funcionarios para el uso.
- Las contraseñas serán asignadas por el Administrador de la Base de Datos en el momento en que el funcionario desee activar su cuenta, previa solicitud al responsable de acuerdo con el procedimiento generado.
- En caso de olvido de contraseña de un funcionario, será necesario que se presente con el Administrador de la Base de Datos para reasignarle su contraseña.

- Para efecto de creación de una cuenta de usuario en cualquier software o aplicación de la empresa EMDUPAR S.A. E.S.P. el área de Recursos Humanos o el jefe inmediato deberá enviar un correo a soporte@emdupar.gov.co, especificando el nombre, cedula y cargo del funcionario a crear la cuenta.
- La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales, con letra mayúscula al inicio.

## 5.19. ANTIVIRUS

- Todos los equipos de cómputo de EMDUPAR S.A. E.S.P. deberán tener instalada una Solución Antivirus.
- Periódicamente se hará el rastreo en los equipos de cómputo de EMDUPAR S.A. E.S.P., y se realizará la actualización diaria automática de las firmas de antivirus proporcionadas por el fabricante de la solución antivirus en los equipos conectados a la Red.

## 5.20. FIREWALL

- La solución de seguridad perimetral debe ser controlada con un Firewall por Hardware (físico - FORTIGATE) que se encarga de controlar la entrada y salida del internet, puertos y conexiones, es decir, de permitir el paso y el flujo de datos entre los puertos, ya sean clientes o servidores.
- La División de sistemas de información establecerá las reglas en el Firewall necesarias bloquear, permitir o ignorar el flujo de datos entrante y saliente de la Red.
- El firewall debe bloquear las “conexiones extrañas” y no dejarlas pasar para que no causen problemas.
- El firewall debe controlar los ataques de “Denegación de Servicio” y controlar también el número de conexiones que se están produciendo, y en cuanto detectan que se establecen más de las normales desde un mismo punto bloquearlas y mantener el servicio a salvo.

- Controlar las aplicaciones que acceden a Internet para impedir que programas a los que no hemos permitido explícitamente acceso a Internet, puedan enviar información interna al exterior (tipo troyanos).

## 5.21. REDES PRIVADAS VIRTUALES (VPN)

- Los usuarios móviles y remotos de EMDUPAR S.A. E.S.P. podrán tener acceso al a red interna privada cuando se encuentren fuera de la Empresa alrededor del mundo en cualquier ubicación con acceso al Internet público, utilizando las redes privadas VPN (FortiClientOnline) habilitadas por el Área de Sistemas.
- La División de Sistemas de Información serán los encargados de configurar el software necesario y asignar las claves a los usuarios que lo soliciten.

## 5.22. CONECTIVIDAD A INTERNET

- La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Todos los empleados de EMDUPAR S.A. E.S.P. tienen las mismas responsabilidades en cuanto al uso de Internet.
- El acceso a Internet se restringe exclusivamente a través de la Red establecida para ello, es decir, por medio del sistema de seguridad con Firewall incorporado en la misma. No se debe realizar descargas no autorizadas, ni acceder a páginas de videos en línea o en tiempo real, películas, juegos, pornografía y demás que entorpezcan las labores diarias y consuman el ancho de banda del canal de internet de la empresa.
- Entre las medidas de seguridad se encuentra configurado para restringir algunas palabras y sitios de Internet; por lo que pueden existir palabras o sitios que a pesar de ser inofensivos tendrán negado el acceso; en este caso, los funcionarios podrán notificar esta eventualidad para que sea resuelta a la brevedad posible.

### 5.23. RED INALÁMBRICA (WIFI)

#### 5.23.1 Acceso a Funcionarios de Las Empresas:

- La red inalámbrica (Wifi Emdupar) es un servicio que permite conectarse a la red de EMDUPAR S.A. E.S.P. e Internet sin la necesidad de algún tipo de cableado. La Red inalámbrica le permitirá utilizar todos los servicios de Red, en las zonas donde allá cobertura de Wifi.
- La División de Sistemas de Información, es la encargada de la configuración, administración, habilitación y/o bajas de usuarios en la red inalámbrica de la empresa.
- La División de Sistemas de Información determinará las medidas pertinentes de seguridad para usar las redes inalámbricas.
- El área de Sistemas de Información se reserva el derecho de limitar los anchos de banda de cada conexión según sea necesario, para asegurar la confiabilidad y desempeño de la red y de esta manera garantizar que la red sea compartida de una manera equitativa por todos los usuarios de la Empresa.
- No se permiten la operación ni instalación de “puntos de acceso” (access points) conectados a la red cableada de EMDUPAR S.A. E.S.P. sin la debida autorización por parte de la División de Sistemas de Información.

#### 5.23.2 Acceso a Invitados:

- La Red inalámbrica de Invitados le permitirá utilizar los servicios de Internet, en las zonas de cobertura de la Empresa.
- Para acceder a la red WIFI como invitado debe garantizar la persona que el computador tenga instalado un software antivirus actualizado y se le debe configurar una dirección IP fija temporal, la cual al final del uso debe ser retirada por el personal de la División de Sistemas de Información.

## 6. REGISTROS

Comunicaciones internas.
Copias de respaldo de la información.

Inventarios de equipos.
Listado maestro de documentos Internos y Externos.

## 7. DOCUMENTOS DE REFERENCIA

- LEY 1474 DE 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- DECRETO 4632 DE 2011: Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.
- LEY ESTATUTARIA 1581 DE 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.
- NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001:20013. 2013-12-11. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.
- MANUAL GOBIERNO EN LÍNEA 3.1 Ver 2014-06-12: Para la Implementación de la Estrategia de Gobierno en Línea, Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.
- LEY 1712 DE 2014: Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones.
- DECRETO 2573 DE 2014: Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
- DECRETO 103 DE 2015: Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- DECRETO 1494 DE 2015: Por el cual se corrigen yerros en la Ley 1712 de 2014.
- DECRETO 1499 DE 2017: Modelo Integrado de Planeación y Gestión (MIPG). Dimensión: Gestión con Valores para Resultados.

## 8. CONTROL DE CAMBIOS

| VERSIÓN | FECHA | RESPONSABLE | DESCRIPCIÓN |
|---|---|---|---|
| **01** | **15-12-09** | GESTION DE INFORMATICA | ELABORACION DEL DOCUMENTO |
| **02** | **19-07-11** | GESTION DE INFORMATICA | • SE REALIZO CAMBIO EN TODA LA ESTRUCTURA Y FORMA DEL PRESENTE PROCEDIMIENTO,<br>• SE ANEXO LAS OPCIÓN DE APROBACIÓN. SEGÚN FORMATO (FO-GD-01) "ACTA DE REUNIÓN 19-07-11" |
| **03** | **01-06-18** | GESTION DE INFORMATICA | • SE REALIZO ACTUALIZACION DEL PRESENTE PROCEDIMIENTO. |