1. GENERALIDADES.

La Unidad de TI de Cajamag a través de estos lineamientos busca minimizar factores de riesgos a la información como activo de la Corporación.

2. RESPONSABILIDAD.

El Jefe Unidad TI será el responsable de establecer los lineamientos a tener en cuenta para salvaguardar la información de la Corporación

3. POLÍTICAS GENERALES.

3.1 Se prohíbe la Instalación, Reproducción, uso de programas o recursos para los cuales no exista una licencia o autorización de uso válido a nombre de la empresa.

3.2 La Caja se reserva el derecho a auditar, vigilar y fiscalizar los sistemas de correspondencia electrónica y todos los servicios computarizados para garantizar que su propiedad sea utilizada sólo para propósitos y gestiones relacionadas con el trabajo. Estas auditorías se realizarán periódicamente, al azar o cuando exista una investigación sobre una situación en particular. Al personal de la Empresa no le alberga expectativa de intimidad con relación a cualquier información, documento, mensaje creado, recibido o enviado a través del sistema de correo electrónico (E-mail) de carácter personal.

3.3 Todos los archivos que se creen en los computadores serán guardados en el perfil de dominio de cada usuario con el fin de protegerlos mediante los mecanismos de resguardo (backup) existentes. En este perfil solo deben ser almacenados los archivos de trabajo; todo contenido diferente a archivos de Excel, Word, Power Point, Access, Publisher, Corel Draw, Corel Photo Paint, etc. Será eliminado es decir archivos de Música, Videos, Fotografías diferentes a las Institucionales, etc. Serán borrados de las estaciones.

3.4 Cada Usuario de la Red de datos posee un Nombre de usuario ("Login") el cual consistirá en una estructura compuesta por su nombre seguido de un punto (.) y su apellido. Ej. El usuario Pedro Pérez poseerá el login pedro.perez en minúscula. Así mismo cada usuario posee un perfil de seguridad, el cual determina sus niveles de acceso y permisos en la Red de datos. Este perfil lo asigna la Unidad de TI. Al ser contratado un nuevo miembro de la Corporación, la Unidad de Talento Humano deberá informar a la Unidad de TI, con el fin de generar el login y el Perfil para el nuevo usuario siempre y cuando este deba ingresar al sistema.

3.5 El uso de una Clave de acceso ("password") no impedirá que se audite el sistema y no significa que el usuario albergue expectativa de intimidad alguna con relación a la información almacenada en el computador asignado o en cualquier otro. Las contraseñas deben mantenerse en estricta confidencialidad ya que son personales e intransferibles y se cambiarán cada ciento ochenta (180) días. La misma será de por lo menos ocho (8) caracteres de longitud y deberá ser una combinación de caracteres alfanuméricos (letras mayúsculas, minúsculas, números, símbolos) en cualquier proporción o arreglo. La contraseña utilizada por el usuario no podrá repetirse cuando expire la validada en el sistema. Al momento de intentar ingresar al sistema, el usuario tendrá la oportunidad de equivocarse 6 veces; en el séptimo intento la cuenta será bloqueada por espacio de 20 minutos; al cabo de este tiempo, el usuario podrá intentar nuevamente. Cada Usuario debe ingresar con su Nombre de Usuario y Password a las estaciones; en caso de que el usuario se levante de su puesto, deberá bloquear su estación por medio de la combinación de teclas Ctrl + Alt + Suprimir. Para el caso de que se requiera el préstamo de la estación, el nuevo usuario deberá ingresar con su propio Nombre de usuario y password.

3.6 Se prohíbe modificar los privilegios de acceso a las redes internas o externas para obtener acceso no autorizado a dichos recursos.

3.7 Se prohíbe el envío fuera de la Oficina de documentos electrónicos o mensajes por medio del correo electrónico (e-mail) que contengan información confidencial.

3.8 Se prohíbe el envío o recibo de mensajes de correo electrónico entre el personal de la Empresa y personas ajenas a la misma en los cuales se divulguen, comenten o expresen hechos, opiniones u otra situación o asuntos internos de la Empresa, que puedan poner en entredicho la reputación y la imagen de esta.

3.9 La descarga de Software (*.exe, *.com, *.bat, *.mp3, *.mp4, *.aac, *.ogg, *.mpg), y cualquier otro tipo de software ejecutable, de audio, de video queda restringida; para el caso que se requiera la descarga de alguno de estos tipos de archivos, se debe enviar la solicitud por el sistema de solicitudes debidamente justificado. De la misma forma se prohíbe la instalación o uso de programas de descarga masiva o P2P. Quedan Restringidos además todo tipo de programas o páginas web de chat o redes sociales y aplicaciones para conexiones VPN como Thor.

3.10 No se podrá modificar ni archivar la información propiedad de la Empresa con el propósito de impedir que alguien pueda leerlos, entenderlos o utilizarlos. Tampoco se podrá alterar el nombre del usuario u otra

información que se utilice regularmente para identificar la información, mensajes o archivo. En caso de que algún usuario asigne contraseñas o codifique la información a fines de evitar que otras personas puedan leerla, este proveerá todos los datos para lograr acceso a los archivos al momento de su creación. La Empresa está facultada para decodificar la misma o restituirla a su condición original.

3.11 Se prohíbe modificar los parámetros y configuración adoptados por la Unidad de TI en los computadores de la Empresa, en la capacidad de recibir llamadas telefónicas, conexión remota o cualquier otro tipo de acceso no autorizado en la red.

3.12 Todo Nuevo Software que la Caja desee adquirir debe ser evaluado por la Unidad de TI a fin de establecer Compatibilidad, Seguridad, y Coherencia con respecto a la infraestructura, que maneja la Caja.

3.13 Ningún usuario realizará tareas de instalación de equipo, programas (software) ni de reparación. Solamente el personal autorizado por la Unidad de TI podrá instalar y configurar los equipos de computo.

3.14 Ningún usuario llevará alimentos ni bebidas a las áreas de trabajo donde los equipos de computadoras estén localizados.

3.15 Cualquier movimiento de equipos, así como de sus periféricos deberá ser coordinado con el personal de la Unidad de TI.

3.16 Cualquier movimiento de traslado de puesto o quipos de trabajo deberá ser coordinado con la Unidad de TI.

3.17 Con el fin de lograr la mayor uniformidad, antes de la adquisición de computadores, redes, servicios electrónicos internos y Software, deberá contarse con el asesoramiento de la Unidad de TI.

3.18 Al finalizar el día los usuarios deberán retirar sus claves de acceso de los terminales o computadoras y apagar todos los equipos electrónicos en su área de trabajo cuando el servicio así lo requiera.

3.19 En caso de emergencia cada usuario es responsable de tomar las medidas necesarias para proteger el equipo bajo su uso.

3.20 En caso de que se dé una tormenta eléctrica se deberán desconectar de los equipos de trabajos de las redes de voz, datos y eléctrica.

3.21 Se prohíbe la apertura de cualquier equipo de cómputo (computadores, teléfonos IP, impresoras, switch, servidores, etc.) para su manipulación o

extracción de hardware excepto el personal autorizado por la Unidad de T.I.

3.22 Se prohíbe la conexión de equipos de cómputo personales (computadores, teléfonos IP, impresoras, switch, servidores, etc.) a la red interna de la Caja sin la previa autorización de la Unidad de TI.

3.23 Se prohíbe llevarse equipos de cómputo (computadores, teléfonos IP, impresoras, switch, servidores, etc.) fuera de la Caja sin la previa autorización de la Unidad de TI y la realización del procedimiento de salida de activos.

3.24 Se prohíbe bajar información (download) de los servicios de Internet sin la debida autorización del Director o de la persona que éste designe a cargo de la Unidad de TI. Se exceptúa de esta prohibición al personal técnico encargado de brindar mantenimiento a los computadores, redes, servicios electrónicos internos y a la red Internet.

3.25 Se prohíbe utilizar el sistema para acceder y almacenar información en cuentas de correo electrónico distintas a las cuentas provistas por la empresa, excepto al Director Administrativo, Jefes de División, Auditora Interna o cualquier otro personal autorizado.

3.26 Se prohíbe el envío de copias de mensajes de correspondencia electrónica con información confidencial sin el consentimiento del remitente original.

3.27 Se prohíbe guardar, enviar y recibir mensajes en exceso de la cuota asignada a cada usuario en el servidor de la Empresa.

3.28 Se prohíbe la reproducción maliciosa o voluntaria de virus, envío de correo que no sea oficial, envío de material ofensivo, ilegal o pornográfico o de cualquier otra índole no autorizada.

3.29 Cada usuario será responsable de sus actos y conducta al acceder a Internet o al utilizar el correo electrónico.

4. BACKUPS:

Son generadas copias de seguridad de las bases de datos de forma diaria, además de los programas fuentes de todos los aplicativos y los archivos de configuración del sistema. CAJAMAG, define los siguientes tipos de backups:

4.1 Backup Incrementales

El software veeam backup copia los datos que han variado desde la última operación de backup de cualquier tipo. Se utiliza la hora y fecha de modificación estampada en los archivos, comparándola con la hora y fecha de la última copia de seguridad.

4.2 Backup Totales

Constan de aquellos Backup que se realizan a los servidores, los cuales son archivados y almacenados durante 1 mes para los servicios de Bases de Datos y 7 días para los servicios diferentes a bases de datos, en la política de backup, el veeam backup se encarga de gestionarlos diariamente.

5. PERMISOS Y CONTROLES DE ACCESO:

5.1 Todos los permisos para acceder a los sistemas se define mediante una estructura de roles que establece funciones específicas de acuerdo a niveles de acceso, entregados desde la administración central de cada aplicación a través de código de usuario y password encriptados en sus respectivas bases de datos. Los roles se establecen de acuerdo a unas necesidades básicas atendiendo el criterio especificado en las funciones de cada empleado, su ámbito de trabajo y el software que requiere usar para el cumplimiento de su labor.

5.2 **Los Controles de Acceso**

5.3 Se hará una depuración cada 6 meses de las cuentas existentes identificado cuales deben quedar activas e inactivar las que según sea el caso pertenezcan a usuarios que ya no estén en la Corporación.

5.4 Para todas las áreas se realizará la inactivación de cuentas de dominio, cuando los trabajadores salgan de vacaciones, licencias, permisos o demás procedimiento que justifique la ausencia en el puesto de trabajo. Esto se realizará quincenalmente, según las notificaciones respectivas del Jefe de Área del cual haga parte el empleado.

6. Registros de eventos del sistema:

6.1 Cada uno de los aplicativos de CAJAMAG cuenta con un registro individual de actividades de usuarios, haciendo posible una auditoría efectiva en el seguimiento a las actividades de cada miembro del sistema

7. OTRAS DISPOSICIONES

7.1 Queda prohibido el manejo o transmisión de material obsceno, profano u ofensivo a través del sistema de computadores o del sistema de comunicación electrónica de la Empresa. Esto incluye, a modo de ejemplo, acceso a material erótico, bromas de cualquier forma o cualquier comentario o chiste que pueda violar la política contra el hostigamiento sexual o laboral.

7.2 Se prohíbe el uso de programas de charlas ("chats"), excepto los autorizados por la Dirección o su representante autorizado.

7.3 La política adoptada para el uso de Internet será revisada periódicamente en caso de que surjan nuevas necesidades, únicas y particulares de la Empresa. Estas se incorporarán y se hará formar parte de estas guías todos aquellos documentos, memorandos, instrucciones, manuales o políticas que se notifiquen de tiempo en tiempo y que estén relacionadas al uso de los computadores de la Empresa.

7.4 Cada empleado de la Empresa es responsable de conocer dichas órdenes administrativas sobre el uso y manejo del sistema de informática.

7.5 Todo empleado será responsable de informar por escrito al Director Administrativo o Jefe de la Unidad de TI sobre cualquier situación, incidente, problema de seguridad, acceso indebido o violación voluntaria o involuntaria de estas normas para el uso de los computadores o redes de la Empresa.

8. MEDIDAS DISCIPLINARIAS

8.1 El incumplimiento de las disposiciones de este reglamento estará sujeto a investigación administrativa y a la imposición de las medidas disciplinarias correspondientes.

9. VIGENCIA

9.1 Este reglamento entrará en vigor a partir de la fecha de aprobación.

9.2 La Unidad de TI velará por el licenciamiento de los productos y registrará las licencias en sus respectivas compañías.

9.3 Toda compra e instalaciones de hardware y software, deben ser certificadas y verificadas por la Unidad de TI.

Tabla de Control de Cambios		
Versión	Cambio	Fecha
2	Se cambió la periodicidad por generar Backup de las bases de datos de forma diaria, además de los programas fuentes de todos los aplicativos y los archivos de configuración del sistema. Se definieron los tipos de backups en: **Backup Incrementales** el cual Consta de 6 Backup diarios, cuyo periodo de caducidad es de 15 días para el Software de Automatización de Backup Tivoli Storage Manager, estos Backup son almacenados cada 12 horas en los Storage Pool de discos duro gestionados por el Tivoli Storage Manager a través de la ruta "/datos/nombre_del_servidor/diario/incrementales". **Backup Diferenciales** que consta de 6 Backup diarios, con caducidad es de 15 días para el Software de Automatización de Backup Tivoli Storage Manager, almacenados cada 12 horas en los Storage Pool de discos duro gestionados por el Tivoli Storage Manager y a diferencia de los Backup Incrementales, estos son almacenados en la ruta "/datos/nombre_del_servidor/diario/diferenciales". **Backup Totales** que son archivados y almacenados durante 6 meses para todos los servicios dentro de la política de Backup semanales y 5 años solo para los servicios de Bases de Datos en la política de backup mensuales, el Tivoli Storage Manager se encarga de gestionarlos cada lunes de la semana para los Backup semanales y el ultimo lunes del mes para los Backup mensuales, cabe mencionar que en diferencia de los otros Backup, estos son almacenados en Cintas magneticas a través de la ruta "/datos/nombre_del_servidor/semanal" para los semanales y mensuales.	27/08/2013
	En el Subtítulo Permisos y Controles de Acceso en el ítem de Controles de Acceso se cambió los aplicativos enunciados por "todos los Aplicativos".	
	Se hicieron cambios de forma que no afectan la esencia de las políticas y del documento en general.	

ELABORÓ	REVISÓ	APROBÓ
JHONATAN CASTRO POLO **JEFE UNIDAD DE T.I (E)** **Fecha de elaboración:** 06/09/2021	GISSELLA MARGARITA MENDIVIL RODRIGUEZ **JEFE UNIDAD PLANEACION Y ESTADISTICAS** **Fecha de revisión:** 09/09/2021	WILMER JOSE PALMA SANTODOMINGO **JEFE DIVISION ADMINISTRATIVA** **Fecha de aprobación:** 27/09/2021