1. GENERALIDADES.

La Oficina de Estrategias 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 General de Estrategias de TI será responsable de establecer los lineamientos a tener en cuenta para salvaguardar la información de la Corporación.
- Jefes de dependencias: Asegurar que su personal conozca y cumpla las políticas; tramitar altas, movimientos y retiros; solicitar accesos y su revocación.
- Usuarios: Cumplir estas políticas; custodiar credenciales; reportar incidentes o situaciones de riesgo.

3. POLÍTICAS GENERALES.

- 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.
- 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) o cualquier otra herramienta de comunicación de carácter personal.
- Todos los archivos que se creen en los computadores serán guardados en el perfil de dominio de cada usuario, quien será responsable de respaldar sus documentos corporativos en las herramientas de almacenamiento autorizadas por la Oficina de Estrategias de TI.
- Cada Usuario de la Red de datos posee un Nombre de usuario ("Login") el cual consistirá en una estructura compuesta por el

formato nombre.apellido 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 Oficina de Estrategias de TI. Al ser contratado un nuevo miembro de la Corporación, la Unidad de Talento Humano deberá informar a la Oficina de Estrategias de TI, con el fin de generar el login y el perfil para el nuevo usuario siempre y cuando este deba ingresar a cualquiera de los sistemas de la entidad o el líder el proceso en caso de ser personal por otro modelo contractual.

- El acceso a los sistemas y datos se basará en el principio de 'mínimo privilegio'. A cada usuario se le asignarán únicamente los permisos estrictamente necesarios para desempeñar las funciones de su cargo. Los derechos de acceso serán revisados anualmente.

- Contraseñas y bloqueo de sesión: Las contraseñas son personales e intransferibles y deben mantenerse en estricta confidencialidad, Longitud mínima 12 caracteres; se recomienda combinar mayúsculas, minúsculas, números y símbolos y no reutilizar entre sistemas. Se aplicará bloqueo automático tras 5 intentos fallidos por 15 minutos. El uso de MFA es obligatorio para sistemas críticos que tengan incorporado esta funcionalidad y correo institucional (ver 5.3). Siempre que el usuario se aleje del puesto de trabajo, deberá bloquear su estación.

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

- Se prohíbe el envío fuera de las Oficinas de la entidad de documentos electrónicos o mensajes por medio del correo electrónico (e-mail) que contengan información confidencial y/o clasificada de la Empresa.

- Se prohíbe el envío o recibo de mensajes a través de correo electrónico, chats u otros medios de comunicación 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.

- 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.

- 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.

- Se prohíbe modificar los parámetros y configuración adoptados por la Oficina de Estrategias 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.

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

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

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

- Cualquier movimiento de traslado de puesto que implique puntos de red o equipos de trabajo, así como de sus periféricos deberá ser coordinado con la Oficina de Estrategias de TI.

- Los equipos de cómputo de la entidad deben conectarse a la red eléctrica regulada. En caso de no tener red eléctrica en el área, se debe disponer de un regulador externo.

- 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 Oficina de Estrategias de TI.

- Al finalizar el día los usuarios deberán apagar todos los equipos de cómputo y/o electrónicos en su área de trabajo cuando el servicio así lo requiera.

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

- En caso de ser requerido durante una tormenta eléctrica, se deberán desconectar de los equipos de trabajos de las redes de voz, datos y eléctrica.

- 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 Oficina de Estrategias de T.I.

- 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 Oficina de Estrategias de TI.

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

- Se prohíbe utilizar el sistema para acceder y almacenar información de la entidad 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.

- Es responsabilidad de cada Jefe de área o Unidad solicitar a la Oficina de Estrategias TI la activación de la red virtual privada – VPN, que permite al teletrabajador conectarse de manera segura a la red de datos de la empresa.

- Todo el personal que trabaje de forma remota debe garantizar la seguridad de su entorno de trabajo doméstico, incluyendo la protección de la red Wi-Fi con contraseñas robustas y el uso obligatorio de la VPN corporativa para acceder a los recursos internos de la empresa. Nota: En caso de utilizar equipos de propiedad personal para las actividades de teletrabajo, se deben cumplir con los lineamientos de seguridad que determine la Oficina de Estrategias TI para este tipo de dispositivos.

- 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.

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

- Todos los empleados deben bloquear la sesión de su equipo siempre que se alejen de su puesto de trabajo, sin importar la duración de la ausencia.

- Control de acceso físico: Para ingresar a las instalaciones de CAJAMAG, toda persona deberá realizar la marcación biométrica como mecanismo de control y verificación de acceso.

- Áreas restringidas: Las áreas que albergan servidores o equipos de comunicaciones son de acceso restringido; solo podrá ingresar el personal autorizado por la Oficina de Estrategias de TI y todo acceso deberá registrarse en el sistema de control de acceso.

- Es obligatorio el uso de autenticación de doble factor (2FA/MFA) para acceder a los sistemas que lo requieran. Cada usuario deberá configurar y mantener activo el segundo factor y reportar intentos sospechosos o compromiso de credenciales. Además, la activación de VPN deberá ser solicitada por la Jefatura de área a la Oficina de Estrategias de TI.

- Queda estrictamente prohibido cargar, pegar o introducir información confidencial o interna, datos personales (Ley 1581 de 2012) o propiedad intelectual (p. ej., código fuente, estrategias) en herramientas de IA generativa públicas (p. ej., versiones gratuitas de ChatGPT, Gemini u otras) salvo las autorizadas por el área de Estrategias de TI.

- Queda prohibido el uso de servicios web de procesamiento de PDF para documentos con información confidencial o interna, datos personales, información financiera/contractual/legal, propiedad intelectual, código fuente, diagramas de arquitectura, políticas internas o información de proveedores. Para estos casos deberán usarse herramientas aprobadas por la Oficina de Estrategias de TI.

4. BACKUPS:

Se realizan copias de seguridad de los servidores con la periodicidad definida según la criticidad y el tipo de sistema. La oficina estrategia de TI establece respaldos incrementales, en los que la herramienta de copias de seguridad guarda únicamente los cambios desde la última copia utilizando la fecha y hora de modificación de los archivos, y respaldos totales, consistentes en copias completas de los servidores, cuya retención y frecuencia se determinan en la política vigente aplicable a cada categoría de servicio.

5. PERMISOS Y CONTROLES DE ACCESO:

5.1 Todos los permisos para acceder a los sistemas se definen mediante una estructura de roles que establece funciones específicas de acuerdo con niveles de acceso, entregados desde la administración central de cada aplicación. Los roles se establecen de acuerdo con 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 **Revisión y depuración de cuentas**

5.2.1 Anualmente se realizará la depuración de las cuentas del dominio. Las cuentas de personas que no se encuentren laborando en la Corporación serán deshabilitadas y trasladadas a la Unidad Organizativa "Retirados", conservando identidad y datos asociados por 12 meses para continuidad, auditoría o requerimientos internos; el período podrá extenderse cuando lo exija un proceso o requerimiento legal.

5.2.2 Para todas las áreas se realizará la inactivación de cuentas de dominio, cuando existan ausencias justificadas (vacaciones, licencias, permisos), conforme a notificaciones de la Unidad de Talento Humano, para el personal con tipo de contratación diferente a la directa con la corporación se realizará según las notificaciones del líder del área a la que pertenezcan.

6. REGISTROS DE EVENTOS DEL SISTEMA:

- 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.

- La Oficina de Estrategias TI debe gestionar los mantenimientos preventivos y correctivos de la infraestructura del centro de cómputo y equipos de red.

7. OTRAS DISPOSICIONES

- 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.

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

- 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.

- Cada empleado de la Empresa es responsable de conocer dichas órdenes administrativas sobre el uso y manejo de los sistemas de información y redes de la entidad.

- Todo empleado será responsable de informar por escrito al Director Administrativo o Jefe General de Estrategias 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.

- Todo empleado (de nómina, contratista, en misión y/o practicante) debe aceptar dentro de sus obligaciones la cláusula de confidencialidad sobre la información a la que tengan acceso y aceptar el cumplimiento de las políticas de seguridad de la información institucionales.

8. MEDIDAS DISCIPLINARIAS

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

9. VIGENCIA

- Este reglamento entrará en vigor a partir de la fecha de aprobación.
- La Oficina de Estrategias de TI velará por el licenciamiento de los productos y registrará las licencias en sus respectivas compañías.

- Toda compra e instalaciones de hardware y software deben ser certificadas y verificadas por la Oficina de Estrategias de TI.