1. OBJETIVO

Proveer los lineamientos y controles para fortalecer las estrategias de seguridad de la información, así como los mecanismos a emplear para su comunicación y divulgación a los empleados de la Compañía, garantizando la estabilidad de los servicios informáticos, incrementando la disponibilidad, confidencialidad e integridad de la información de la compañía y protegiendo la imagen de la Compañía.

2. ALCANCE

Las políticas definidas en el presente documento aplican a todos los empleados, contratistas o cualquier tercero que utilicen recursos informáticos de la Compañía.

3. ACCESO A LA INFORMACIÓN

a. Las cuentas y contraseñas o cualquier mecanismo de acceso que le sean otorgados a un empleado son de su responsabilidad y no deben ser divulgados a ninguna otra persona, a menos que exista un requerimiento legal. De acuerdo con lo anterior, los empleados no deben tener cuentas y claves de otros empleados que puedan permitirles accesos no autorizados e indebidos.
b. Cada empleado es responsable de todas las actividades llevadas a cabo con sus cuentas y contraseñas.
c. Los empleados solo deben acceder a la información y los servicios informáticos estrictamente necesarios para el correcto desempeño de sus funciones en la Compañía.
d. El jefe de departamento que tenga a su servicio contratistas temporales o permanentes o cualquier tercero que requiera el acceso a información específica o servicio informático, deberá autorizar solo el acceso indispensable a través de solicitud formal al departamento de Sistemas.
e. Todos los privilegios para el uso de los sistemas de información de la Compañía deben terminar inmediatamente el empleado finaliza su vinculación laboral.
f. Los contratistas o terceros solo deben tener privilegios durante el período de tiempo requerido para llevar a cabo las funciones previamente autorizadas.
g. Los supervisores de cada área deben notificar al departamento de Sistemas cualquier novedad de los movimientos de los empleados y contratistas de la compañía.
h. 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.
i. Ningún tipo de información de la Compañía podrá ser eliminada, ni copiadas a dispositivos de almacenamiento personales, ya que cuenta con protocolos de seguridad mediante el Antivirus de la compañía.
j. Los empleados son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la Compañía y por la Ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.
k. Los empleados y contratistas no deben suministrar información de la Compañía a ninguna entidad externa sin las autorizaciones respectivas. Ante cualquier solicitud, deberán contactar al departamento legal de la Compañía.
l. Los empleados deben firmar y renovar cada año, un acuerdo de cumplimiento de la seguridad, la confidencialidad y el buen manejo de la información.
m. Cuando el empleado finaliza la prestación de sus servicios a la Compañía, se compromete a entregar toda la información respectiva de su trabajo realizado.

n. Una vez retirado el empleado, debe comprometerse a no copiar, ni utilizar, ni comercializar, ni divulgar la información generada o conocida durante la gestión en la Compañía, directamente o a través de terceros.

4. SERVICIOS INFORMÁTICOS

a. El sistema de correo electrónico, Internet y programas relacionados licenciados por la Compañía deben ser usados únicamente para la ejecución de las funciones de competencia de cada empleado.
b. La Compañía podrá acceder y consultar en los mensajes del sistema de correo electrónicos, si y solo si la compañía lo requiera y el empleado este desvinculado de la empresa.
c. Los empleados que hayan recibido aprobación para tener acceso a Internet a través de los equipos de la Compañía deberán aceptar, respetar y aplicar las prácticas de buen uso de Internet.
d. Los empleados deben informar inmediatamente al departamento de Sistemas toda vulnerabilidad encontrada en los sistemas o servicios informáticos, presuntas infecciones de virus o programas sospechosos e intentos de intromisión y no deben distribuir esta información interna o externamente.
e. Equipos de cómputo de terceros o personales solo podrán conectarse a algún servicio informático de la Compañía en casos excepcionales, previa autorización del jefe de departamento, con solicitud formal y previa revisión del equipo de cómputo por el departamento de Sistemas.

5. RECURSOS INFORMÁTICOS

a. El departamento de Sistemas debe tener un registro de cada uno de los equipos de propiedad de la Compañía.
b. La protección física de los equipos de cómputo corresponde a quienes en un principio se les asigna y les corresponde notificar al departamento de Sistemas los movimientos, daños o reasignaciones autorizadas en caso de que existan.
c. Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel, equipos de cómputo y dispositivos de almacenamiento, con fin de reducir los riesgos de acceso no autorizado, perdida y daño de la información durante el horario normal de trabajo y fuera del mismo.
d. El departamento de Sistemas o terceros autorizados por éste, son los encargados exclusivos de la realización del mantenimiento preventivo y correctivo de los equipos de cómputo.
e. Por ningún motivo se podrán descargar e instalar programas adicionales en los equipos de cómputo asignados, se deberán respetar los derechos de autor bajo cualquier circunstancia.
f. Ningún equipo de cómputo (Portátil, All One, Torre) debe registrarse como equipaje de viaje. Estos deben llevarse como equipaje de mano.

g. Los empleados no podrán utilizar los equipos de cómputo de la Compañía para intentar obtener acceso a redes externas con fines malintencionados.
h. Todo equipo de cómputo, periférico o cualquier dispositivo electrónico deben adquirirse en coordinación y supervisión del departamento de Sistemas y en posibles casos con el departamento de compras.

6. COMUNICACIONES DE VOZ Y DATOS

a. Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y equipos de cómputo de la Compañía deberán ser considerados y tratados como información confidencial.
b. La conexión entre sistemas internos y otros de terceros, debe ser aprobada y certificada por el departamento de Sistemas, con el fin de no comprometer la seguridad de la información interna de la Compañía.
c. Todas las conexiones a redes externas que accedan a la red interna de la Compañía deben pasar, sin excepción, a través de los sistemas de defensa, verificación de datos, detección de ataques cibernéticos, detección de intentos de intrusión, administración de permisos de circulación y autenticación de usuarios.
d. Los empleados no deben suministrarle ningún tipo de información a terceros desconocidos que los contacten telefónicamente u otro medio argumentando cualquier necesidad específica.

7. ALMACENAMIENTO Y RESPALDO

a. Cada empleado es responsable del respaldo de su información en los equipos de cómputo, siguiendo las indicaciones técnicas dictadas por el departamento de Sistemas.
b. La información que es soportada por la infraestructura de tecnología informática de la Compañía deberá ser almacenada y respaldada de acuerdo con las normas de tal forma que se garantice su disponibilidad.
c. Los respaldos de información de valor o sensible, deben tener un proceso periódico de validación, con el fin de garantizar que no han sufrido ningún deterioro y que se podrán utilizar en cualquier momento.
d. Los medios con respaldos deben almacenarse externamente.

8. SANCIONES

Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo con el reglamento interno de trabajo.

9. CONTROL DE CAMBIOS

Versión revisada No.	**Fecha de revisión:** 04/08/2023	**Fecha de aprobación:** 04/08/2023	**Nueva versión No.** 01

(A) (S)	**Ubicación**	**Descripción del cambio**
(A)	Todo el documento	Emisión del documento y codificación

Elaboró: Antonio Navarro Comas	Revisó: Germán Villegas	Aprobó: Germán Villegas