1. OBJETIVO

Garantizar la integridad, confidencialidad y disponibilidad de la información de Agrícola Automotriz SAS, identificando amenazas y vulnerabilidades y minimizando los riesgos asociados con el fin de asegurar la continuidad del negocio.

2. ALCANCE

Aplica a todos los trabajadores directos o temporales, aprendices, proveedores y terceros de Agrícola Automotriz SAS.

3. DEFINICIONES

3.1 Certificado: Declaración que garantiza la identidad de una organización o la seguridad de un sitio o servidor web.

3.2 Antivirus: Programas especializados en detección y destrucción de virus informáticos.

3.3 Integridad: Propiedad de la información que busca preservar su exactitud.

3.4 Confidencialidad: Propiedad de la información que la hace no disponible o divulgada a individuos, entidades o procesos no autorizados.

3.5 Disponibilidad: Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.

3.6 Virus: Programa informático que se ejecuta en la máquina de cómputo sin previo aviso y que puede corromper programas, archivos de datos y el sistema operativo.

3.7 Seguridad de la información: Conjunto de medidas técnicas, operativas, organizativas y legales que permiten a las organizaciones resguardar y proteger la información, garantizando la confidencialidad.

3.8 Spam: Correo electrónico que se recibe de forma indeseada, generalmente con carácter comercial.

4. REGISTROS

Código	Nombre del Registro	Responsable de generar
N/A	Cláusula de Confidencialidad Trabajadores	Gestión Financiera y Nómina
N/A	Cláusula de Confidencialidad Proveedores y Terceros	Gestión Financiera y Nómina

5. ROLES Y RESPONSABILIDADES

Agrícola Automotriz SAS define los roles y responsabilidades para la implementación, estandarización y mejora de los lineamientos de seguridad descritos en esta política y los documentos asociados al proceso.

ROL / AREA	RESPONSABILIDADES
Alta Dirección	• Proporcionar los recursos necesarios para la implementación y mantenimiento del sistema de gestión de seguridad de la información (Recursos económicos, formación y recursos tecnológicos).
Proveedor Servicios TI / Calidad	• Dar apoyo en la generación de los lineamientos (Manuales, procedimientos y formatos) que permitan el establecimiento y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información en la Entidad. • Analizar, definir, documentar y gestionar el plan estratégico de seguridad de la información y proponer las decisiones que permitan gestionar la seguridad de la información en el marco del cumplimiento de la política y los lineamientos definidos y aprobados por la entidad. • Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información. • Garantizar que los trabajadores y contratistas tomen conciencia de sus responsabilidades en seguridad de la información y las cumplan, además de dar aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos. • Verificar e implementar las medidas de seguridad de la información en la gestión con los proveedores y contratistas de la entidad. • Procurar la protección de la seguridad de la información de todos los activos de la información que puedan verse involucrados en procesos o contratos.
Área de Calidad	• Incluir la seguridad de la información, dentro de los planes de auditoría institucionales.

ROL / AREA	RESPONSABILIDADES
	• Dar apoyo en situaciones de posibles violaciones a las políticas de seguridad de la información.
Jefes de área	• Dar apoyo en las labores de comunicación y sensibilización en seguridad de la información, para difundir la información en todos los niveles de la entidad. • Implementar las políticas y procedimientos de seguridad de la información que se definan como parte del SGSI (Por ejemplo: gestión de activos, gestión de riesgos, entre otros).
Todos los trabajadores y contratistas	• Apoyar a los líderes de proceso en el desarrollo de tareas como gestión de activos y gestión de riesgos. • Cumplir a cabalidad con las políticas y procedimientos de seguridad de la información definidos y aprobados.

6. POLÍTICAS

6.1 POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Agrícola Automotriz S.A.S., con el fin de proteger la confidencialidad, integridad y disponibilidad de los activos de información, se compromete con la implementación, mantenimiento y mejora de las políticas para garantizar la seguridad de la información y el uso adecuado de equipos tecnológicos, dando cumplimiento a la normatividad vigente y aplicable.

Agrícola Automotriz S.A.S., en su propósito de establecer la política de seguridad y privacidad de la información, define los siguientes objetivos:

OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN:

1. Fortalecer la cultura de seguridad de la información en los trabajadores, proveedores, terceros, aprendices y clientes de Agrícola Agricola Automotriz SAS.
2. Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
3. Minimizar el riesgo de todos los procesos de la entidad.
4. Estandarizar los controles tecnológicos necesarios para la protección de los activos de la entidad y para la reducción de los riesgos.

6.2 USO GENERAL Y PROPIEDAD DE LA INFORMACIÓN

Agrícola Automotriz SAS es propietario de toda la información generada y capital intelectual de la Organización. El Proveedor Tecnológico Gestión Franca es administrador de toda información generada o adquirida por bases de datos, servidores y equipos de cómputo de propiedad de la Organización.

- ✓ La información almacenada por el proveedor de informática y tecnología en bases de datos, servidores, o cualquier medio electrónico es propiedad de Agrícola Automotriz SAS de conformidad con la legislación en materia de protección de datos y derechos de autor.

- ✓ La información almacenada electrónicamente en equipos de cómputo o dispositivos propios, alquilados o de terceros seguirá siendo de propiedad de Agrícola Automotriz.

- ✓ Los trabajadores son responsables de ejercer un buen uso de los equipos de cómputo y dispositivos electrónicos suministrados por Agrícola Automotriz SAS.

- ✓ Los trabajadores pueden acceder, usar o compartir la información solicitada por terceros siempre y cuando se encuentren debidamente autorizados y sea necesaria para el cumplimiento de funciones y responsabilidades.

- ✓ De acuerdo a la política de seguridad de la Información del Proveedor Tecnológico, "**Gestión Franca se reserva el derecho de auditar las redes, dispositivos y sistemas de manera periódica validando cumplimento de sus políticas internas por lo que, para propósitos de supervisión y mantenimiento de la Red, monitorean los equipos, sistemas y tráfico de la Red, en búsqueda constante de fuentes de amenazas y vulnerabilidad que pueden afectar los activos de información de la Organización**".

- ✓ La Organización define como información reservada para especial protección, toda información que contenga la operación de la Organización en especial la relacionada con los procesos y procedimientos a las que se tenga acceso de acuerdo a las funciones a realizar dentro de los roles y responsabilidades de los trabajadores, para esto toda contratación que tenga la Agrícola Automotriz SAS debe tener un acuerdo de Confidencialidad donde se define que la información reservada es:

    - ➢ Cifras
    - ➢ Procesos
    - ➢ Listados
    - ➢ Planes de negocio
    - ➢ Información relacionada con la estructura corporativa.
    - ➢ Servicios de la compañía
    - ➢ Productos
    - ➢ Servicios suministrados y ofrecidos

- Procedimientos internos relacionados con el desarrollo del objeto social de la compañía
- Formatos desarrollados por la compañía tanto para procesos internos como externos
- Información técnica sobre la operación de la compañía
- Toda aquella información que pueda guardar relación con el objeto social de la compañía y los servicios y productos ofrecidos
- Información contenida en las hojas de vida de colaboradores.
- Resultados de pruebas psicotécnicas.
- Memorandos de recomendaciones.
- Bases de datos (clientes), colaboradores, presupuestos, etc.

✓ Quien tenga acceso a la información se compromete a suscribir nuevas cláusulas de confidencialidad o a modificar las existentes, en la medida la Organización declare como tal, nueva información de carácter reservado y que éste deba conocer con ocasión de la ejecución del contrato de trabajo o del vínculo comercial.

✓ Los trabajadores o terceros con acceso a la información deben reportar de inmediato al jefe de área y proveedor de tecnología el robo, pérdida o divulgación no autorizada de información de propiedad de Agrícola Automotriz SAS.

✓ Por motivos de seguridad, seguimiento y mantenimiento de la red el proveedor de tecnología e informática podrán monitorear los equipos, sistemas y tráfico de red en cualquier momento.

✓ El receptor de la información asume la obligación de no usar, explotar, divulgar, revelar, exhibir o adquirir sin autorización de la Organización, en beneficio propio o de un tercero, la información o documentación reservada a la que tenga acceso, en consecuencia reconoce y acepta que Agrícola Automotriz SAS es titular exclusivo de cualquier derecho sobre la información y documentación a la que tenga acceso con ocasión del contrato de trabajo o el vínculo comercial que tenga con la Organización. Igualmente, reconoce y acepta que respecto de la información mencionada no tiene derecho alguno, por lo cual se obliga a no copiarla, a no duplicarla, a no sustraerla y a no comunicarla, en favor de terceros, ni a usarla para sí, durante el tiempo que dure la relación laboral o comercial ni en momento posterior a la terminación esta. Así mismo, el receptor de la información se obliga, a que, una vez terminada la relación laboral o comercial existente con la Agrícola Automotriz SAS devolverá toda la documentación que se le haya dado en ejecución del mismo.

6.3 POLITICA DEPURACIÓN DE BASES DE DATOS

Agricola Automotriz SAS, dando cumplimiento a la Ley 1581 de 2012, establece mediante la política de depuración de bases de datos los responsables de actualizar, corregir y eliminar registros de datos erróneos de las bases de datos utilizadas por la compañía así:

- ✓ Departamento Comercial: Auxiliar Administrativa / Secretaria Comercial.
- ✓ Departamento de Servicio: Auxiliar CRM
- ✓ Departamento Contable: Asistente Contable/Analista de nómina
- ✓ Porsche: Jefe Porsche
- ✓ Departamento Equipos Industriales: Auxiliar Administrativa

La actualización, modificación o eliminación deberá ser reportada al departamento de Calidad y deberá realizarse cada que se requiera o con una periodicidad semestral.

6.4 SEGREGACIÓN DE FUNCIONES

- ✓ Todos los trabajadores que tengan acceso a la infraestructura tecnológica y a los sistemas de información, deben contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y los permisos correspondientes, con el fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información de la Organización.

6.5 USO DE REDES DE DATOS

- ✓ Es responsabilidad del Proveedor Tecnológico Gestión Franca el buen uso y la manipulación de las redes de datos de la Organización, y según sus Políticas Internas.

- ✓ El acceso lógico y físico a los equipos especializados de cómputo como servidores, router etc., deberá ser exclusivo y administrado por Gestión Franca. Para el caso especial de terceros y proveedores de servicios especializados la Organización debe solicitar autorización.

- ✓ La solicitud de creación o modificación de accesos a las redes, se debe hacer utilizando el sistema de gestión de solicitudes (Mesa de Ayuda) de Gestión Franca.

6.6 ACCESO A WIFI

Agrícola Automotriz SAS implementa las siguientes medidas de control para el acceso a WiFi:

- ✓ El acceso a las redes Wifi se debe realizar por autenticación con su respectivo usuario y contraseña.

- ✓ Las redes Wifi para clientes o visitantes se debe realizar mediante accesos independientes a las corporativas.

- ✓ La Organización establece la prohibición de:

- Transmisión de contenido fraudulento, difamatorio, obsceno, ofensivo o de vandalismo, insultante o acosador, sea este material o mensajes.
- Interceptar, recopilar o almacenar datos sobre terceros sin su conocimiento o consentimiento.
- Escanear o probar la vulnerabilidad de equipos, sistemas o segmentos de red.
- Enviar mensajes no solicitados (spam), virus, o ataques internos o externos.
- Obtener acceso no autorizado a equipos, sistemas o programas tanto al interior de la red como fuera de ella.
- Dañar equipos, sistemas informáticos o redes y/o perturbar el normal funcionamiento de la red y sea usada con fines de lucro, actividades comerciales o ilegales, por ejemplo, hacking.
- Ser utilizada para crear y/o la colocar un virus informático o malware en la red.
- Transmitir, copiar y/o descargar cualquier material que viole cualquier ley. Esto incluye entre otros: material con derecho de autor, pornografía infantil, material amenazante u obsceno, o material protegido por secreto comercial o patentes.

6.7 USO DE EQUIPOS DE CÓMPUTO Y DISPOSITIVOS MÓVILES

- ✓ Todos los equipos conectados a la red de la Organización deberán hacerlo utilizando una cuenta valida registrada en el Directorio Activo del proveedor de tecnología Gestión Franca.

- ✓ Ningún usuario debe tener permisos de administrador sobre los equipos de cómputo de Agrícola Automotriz SAS con el propósito de proteger los equipos contra virus y evitar la instalación de software no licenciado o autorizado.

- ✓ No está permitido el uso de computadores personales o ajenos al asignado para la ejecución de las funciones.

- ✓ No está permitido la configuración de correo corporativo en dispositivos que no son propiedad de la Organización.

6.8 ASIGNACIÓN DE USUARIOS Y CONTRASEÑAS

- ✓ El proveedor de tecnología es el encargado de realizar la activación y desactivación de usuarios conforme a su procedimiento.

- ✓ Las contraseñas asignadas a los usuarios son personales e intransferibles.

- ✓ Las contraseñas se deben cambiar periódicamente las cuales se encuentran programadas por política del controlador de dominio y se establece la periodicidad de ejecución cada 30 días.

- ✓ Las contraseñas deben contar con los siguientes parámetros:

  - ➢ Tener una longitud mínima de ocho caracteres.
  - ➢ Incluir caracteres de las siguientes categorías: Mayúsculas (de la A a la Z) / Minúsculas de la (A a la Z). / Dígitos de base 10 del (0 al 9). / Caracteres no alfanuméricos (por ejemplo $, #, %, *).
  - ➢ Se debe cambiar las contraseñas de inicio asignadas durante la creación de usuarios.
  - ➢ No se debe guardar registros en papel o virtual de contraseñas.

6.9 USO DEL CORREO ELECTRÓNICO CORPORATIVO

- ✓ Agrícola Automotriz SAS asignará por medio del proveedor de informática y tecnología, basado en la matriz de roles y perfiles de seguridad de la información una cuenta de correo electrónico a los trabajadores que de acuerdo a las actividades de su cargo lo requieran, dicha cuenta es personal e intransferible.

- ✓ Los usuarios son los únicos responsables de todas las actividades realizadas con sus cuentas de correo, debiendo cumplir en todo momento las normas de uso y de seguridad de la red de datos de la organización.

- ✓ Los correos electrónicos enviados no podrán incluir contenido ofensivo (uso de lenguaje/imágenes vulgares u ofensivas), ni atentar contra la integridad de la organización.

- ✓ Se prohíbe el uso del correo electrónico corporativo para cualquier propósito comercial o financiero ajeno a las funciones propias de Agrícola Automotriz SAS.

- ✓ Se prohíbe divulgar información que incite a la discriminación o a la violencia.

- ✓ Se prohíbe enviar contenido con fines personales y servicios en beneficio propio, de familiares o terceros.

- ✓ Se prohíbe enviar correo tipo SPAM, relacionado con falsos virus, con publicidad de empresas, cadenas de mensajes, etc.

- ✓ Se prohíbe usar la cuenta de correo electrónico de otro usuario o entregar a un tercero la contraseña propia.

- ✓ Se prohíbe falsificar mensajes de correo electrónico.

- ✓ Se prohíbe borrar, copiar o modificar mensajes de correo electrónico de otras personas sin su autorización.

- ✓ Agrícola Automotriz SAS no asume responsabilidad alguna por los contenidos emitidos a través del correo electrónico o por el uso ilegal y mal intencionado por parte de los usuarios.

6.10 ALMACENAMIENTO DE INFORMACION, ESCRITORIO Y PANTALLA DESPEJADOS

- ✓ Toda la información generada por los trabajadores en el cumplimiento de sus funciones debe ser almacenada en las carpetas de los servidores de archivo destinados para ello.

- ✓ Almacenar únicamente información relacionada con sus actividades laborales, en el espacio asignado.

- ✓ Al dejar el equipo de cómputo desatendido, sin excepción se debe utilizar protector de pantalla protegido con contraseña, de modo que al regresar al puesto de trabajo deberá introducirse nuevamente la clave para el acceso al equipo.

- ✓ Se debe apagar el computador al alejarse por períodos prolongados de tiempo o al finalizar la jornada laboral.

- ✓ Es responsabilidad del proveedor de informática y tecnología controlar los derechos de lectura, escritura y modificación para usuarios, preservando siempre los principios de integridad, confidencialidad y disponibilidad de la información.

6.11 INTERCAMBIO DE INFORMACIÓN

- ✓ No está permitido entregar información a terceros sin previa autorización del jefe inmediato y/o Gerente de área según corresponda.

- ✓ Todos los trabajadores, proveedores y terceros están obligados a dar cumplimiento a los acuerdos de confidencialidad establecidos, por lo tanto, serán responsables de la entrega de información no autorizada.

- ✓ Es responsabilidad de los dueños de información sensible no dejar copias impresas o documentos físicos en lugares de fácil acceso a personal no autorizado.

- ✓ La información sensible disponible al público por medio de sitios web deben estar protegidas por sitios seguros.

6.12 PROTECCIÓN CONTRA CÓDIGOS MÓVILES O MALICIOSOS

- ✓ Restringir el uso de los equipos por parte de personas ajenas a las actividades propias de la organización.

- ✓ Se debe contar con una copia de respaldo de los archivos que se almacenan en la red, el proveedor de informática y tecnología es responsable de la ejecución, custodia y almacenamiento de estas copias.

- ✓ Restringir el uso de CD´S, memorias tipo USB y otros medios removibles de origen desconocido.

- ✓ No está permitida la desinstalación y/o desactivación de software y herramientas de seguridad avaladas por el proveedor de informática y tecnología.

- ✓ No está permitido el uso de medios de almacenamiento físico o virtual que no sean de carácter corporativo.

- ✓ No se permite escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar la disponibilidad, integridad y confidencialidad de la información, así como el desempeño de cualquier dispositivo o infraestructura tecnológica de la Agrícola Automotriz SAS.

6.13 CONTROLES DE ACCESO

- ✓ Se utilizan cámaras de video (CCTV) para supervisar el acceso físico de personas a áreas críticas o controladas que resguardan información confidencial.

- ✓ Se debe garantizar que los registros de grabaciones se guardarán al menos durante 45 días.

- ✓ Para los visitantes se debe garantizar que reciben autorización antes de ingresar en las áreas críticas o controladas y estarán acompañados en todo momento por el funcionario encargado de su permanencia.

6.14 GESTION DE INCIDENTES DE SEGURIDAD

Es obligatorio por parte de los usuarios notificar y reportar cualquier evento e incidente de seguridad tan pronto lo detecte o sospeche de ellos. El reporte debe realizarse por medio de un correo electrónico al proveedor de informática y tecnología: mesadeservicios@gestionfranca.com.co

Entre las categorías de incidentes de seguridad que se pueden llegar a presentar se encuentran:

- **Acceso no autorizado:** Comprende todo tipo de ingreso y operación no autorizado a los sistemas, tanto exitosos como no exitosos. Son parte de esta categoría:

  - Accesos no autorizados exitosos, sin perjuicios visibles a componentes tecnológicos.
  - Robo de información.
  - Borrado de información.
  - Alteración de la información.
  - Intentos recurrentes y no recurrentes de acceso no autorizado.
  - Abuso y/o Mal uso de los servicios informáticos internos o externos que requieren autenticación.

- **Código malicioso:** Esta categoría comprende la introducción de códigos maliciosos en la infraestructura tecnológica de la organización. Son parte de esta categoría:

  - Virus informáticos.
  - Troyanos.
  - Gusanos informáticos

- **Denegación del servicio:** Esta categoría incluye los eventos que ocasionan pérdida de un servicio en particular. Los síntomas para detectar un incidente de esta categoría son:

  - Tiempos de respuesta muy bajos sin razones aparentes.
  - Servicio(s) interno(s) inaccesibles sin razones aparentes.
  - Servicio(s) Externo(s) inaccesibles sin razones aparentes

- **Escaneos, pruebas o intentos de obtención de información de la red o de un servidor en particular:** Esta categoría agrupa los eventos que buscan obtener información de la infraestructura tecnológica de la Organización. Comprende:

- Sniffers (software utilizado para capturar información que viaja por la red).
- Detección de Vulnerabilidades.

➢ **Mal uso de los recursos tecnológicos:** Esta categoría agrupa los eventos que atentan contra los recursos tecnológicos por el mal uso. Comprende:

- Mal uso y/o abuso de servicios informáticos internos o externos.
- Violación de las normas de acceso a Internet.
- Mal uso y/o abuso del correo electrónico de la Organización.

➢ **Violación de las Políticas, Normas y Procedimientos de Seguridad Informática reglamentadas.**

6.15 POLITICA DE MANTENIMIENTO DE EQUIPOS DE CÓMPUTO

✓ Anualmente, el proveedor de informática y tecnología ejecutará los mantenimientos preventivos y correctivos de los equipos de cómputo de Agrícola Automotriz SAS, estableciendo el respectivo cronograma.

✓ Los usuarios responsables de los equipos de cómputo no podrán realizar ningún tipo de mantenimiento preventivo, correctivo, ajustes, instalación de software o hardware o cualquier otra actividad que vaya en contra de la integridad física del equipo.

7. SEGUIMIENTO Y EVALUACIÓN

El proveedor de informática y tecnología realizará revisiones periódicas enfocadas en los siguientes aspectos:

- Seguimiento al avance de la implementación de la política de seguridad de la información y uso de equipos tecnológicos.
- Seguimiento y revisión al cumplimiento de los objetivos de la política del Sistema de Gestión de la Seguridad de la Información y uso de equipos tecnológicos.

El incumplimiento a las anteriores políticas dará lugar a las acciones disciplinarias correspondientes, sanciones económicas, terminación de contrato laboral para el caso de empleados o terminación de contrato suscrito entre contratante y contratistas.

8. REVISIÓN Y CONTROL DE CAMBIOS

Versión	Sección	Descripción y naturaleza del cambio	Fecha
02	**6.13**	**Modificación de 30 a 45 días para los registros de grabaciones.**	**29/09/2023**
03	**9**	**Se incluye el numeral 9, control documental.**	**01/07/2025**

9. CONTROL DOCUMENTAL

ELABORADO POR: DAIANNE ROSAS	REVISADO POR: DAIANNE ROSAS	**APROBADO POR: ANDRES GOMEZ**
		
CARGO: JEFE SST/LIDER KAIZEN	CARGO: JEFE SST/LIDER KAIZEN	CARGO: REPRESENTANTE LEGAL

FECHA DE ELABORACIÓN:	FECHA DE REVISIÓN:	FECHA DE APROBACIÓN:
01/07/2025	**01/07/2025**	**15/07/2025**