AGROPECUARIA ALIAR S.A.

POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN
TEC-PO-001

VERSIÓN: 01
FECHA DE EMISIÓN: 01/06/2021

Elaborado Pedro C. Hernández Ingeniero de Software	Revisado Pedro Adarme Coordinador de Comunicaciones y Seguridad Informática	Aprobado René Di Marco Gerente de Tecnología

ÍNDICE

La empresa, en virtud del compromiso con el adecuado tratamiento de datos personales, garantizando además de la salvaguarda y seguridad de la información, el ejercicio del Habeas Data, establece la presente Política aplicable para la seguridad de la información en la organización.

1. OBJETIVO

La presente Política establece las directrices generales para la Seguridad de la Información al interior de AGROPECUARIA ALIAR S.A, con el objetivo de brindar las condiciones de seguridad necesarias que impidan la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento a la información que es tratada por AGROPECUARIA ALIAR S.A.

2. ALCANCE

Aplica en todos los aspectos administrativos, de gestión, logísticos y de control fijados por la empresa, que deben ser cumplidos por los directivos, funcionarios, contratistas, terceros que presten sus servicios, empleados de terceros proveedores que estén regulados por términos contractuales, y en general todas aquellas personas que tengan algún tipo de relación con la manipulación de información en AGROPECUARIA ALIAR S.A, sin que ello constituya o configure subordinación laboral o pérdida de autonomía técnica o directiva respecto de AGROPECUARIA ALIAR S.A.

3. DOCUMENTOS DE REFERENCIA

- Ley de Protección de Datos Personales 1581 de 2012.

4. DEFINICIONES

- **Access Point – AP:** Punto de acceso inalámbrico. Dispositivo que permite la interconexión de computadores y otros equipos electrónicos con capacidades de operar en redes de área local inalámbricas.

- **Active Directory:** Directorio Activo. Es el servicio de directorio implementado por el fabricante de software Microsoft basado en protocolos y estándares, permite bajo una estructura jerárquica, mantener información de los objetos y recursos relacionados con la red como usuarios, computadores, impresoras y políticas de acceso.

- **Activo de Información:** incluye la información estructurada y no estructurada que se encuentre presente en forma impresa, escrita en papel, transmitida por cualquier medio electrónico o almacenada en equipos de cómputo, incluyendo datos contenidos en registros, archivos y bases de datos.

- **Área TI:** Para AGROPECUARIA ALIAR S.A el grupo de profesionales y técnicos a cargo de la infraestructura tecnológica de la compañía, que se encarga de su soporte funcional, del mantenimiento y actualización de la misma.

- **Dueños o responsables de los activos de información:** el dueño del activo de información hace referencia al usuario que crea esta información mediante el uso de algún dispositivo electrónico para almacenar y modificar posteriormente los documentos bajo su dominio, el responsable de la información es el Jefe o Líder de Departamento o Proceso dentro del cual se crea el activo de información.

- **Incidente de seguridad informática:** se define como un evento que atenta contra la Confidencialidad, Integridad y Disponibilidad de la información y de los recursos tecnológicos.

- **Intranet:** Red de computadores en una organización o empresa que, basados en las tecnologías de Internet, como la Web, se interconectan para acceder a información o recursos, a los cuales solo tienen acceso los usuarios de la red local o privada con autorización de un administrador.

- **LAN:** Local Área Network. Interconexión de varios computadores y periféricos. Facilita compartir recursos e intercambiar datos y aplicaciones. El término red de área local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.

- **Malware:** un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el conocimiento de su propietario.

- **SPAM:** mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor y los equipos que soportan el servicio de mensajería o correo electrónico. La acción de enviar dichos mensajes se denomina spamming.

- **Software:** el conjunto de programas de aplicación, sus datos y demás componentes lógicos, que se instalan y se ejecutan sobre un dispositivo físico, por ejemplo, un computador, un teléfono celular, para permitir la interacción y procesamiento de información.

- **Software libre:** denominación que cubre programas y aplicaciones que grupos de desarrolladores, empresas o personas ponen a disposición del público en forma general. Estos programas pueden ser utilizados, copiados, modificados y distribuidos sin necesidad de pagar un licenciamiento o derecho de uso. Suele estar disponible de forma gratuita.

- **Teléfonos inteligentes**: Dispositivo de comunicación móvil que admite correo electrónico, telefonía móvil o celular, navegación web y otros servicios de

información, transporta su información a través de las redes de datos inalámbricas de las empresas de telefonía celular. Ejemplo de estos son los productos de empresas como Apple con el iPhone y Blackberry.

- **TIC:** Tecnologías en Informática y Comunicaciones. El conjunto de programas, redes, servicios y dispositivos tales como computadores y servidores, que, al integrarse en un entorno como una empresa u organización, proveen una infraestructura que facilita el desarrollo de actividades a las personas que la conforman.

- **Virus informático:** un programa no autorizado que se replica por sí mismo, adjuntándose a otros programas, y que se duplica o difunde a través de diversos medios de almacenamiento o incluso a través de las redes y de herramientas como el correo electrónico y de mensajería instantánea generando dificultad en el uso de los recursos del computador.

- **VPN:** Virtual Private Network, Red Privada Virtual, esquema de conectividad en redes de computadores de acceso público, como la Internet, hacia redes empresariales o privadas utilizando métodos de encriptación para proteger la información que se transmite y recibe desde y hacia los computadores de usuario y servidores de la red corporativa.

- **WLAN:** es un sistema de comunicación de datos inalámbrico flexible, utilizado como alternativa a las redes LAN cableadas o como extensión de éstas. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas.

- **FS:** File Server o Servidor de Archivos, es una instancia de un servidor dentro de la red de ordenadores que permite a los usuarios conectados acceder a sus propios recursos de almacenamiento.

- **Usuarios:** Persona que utiliza los servicios prestados por los serviciadores de la compaña para ejercer sus funciones, tales como almacenar información, acceder a Internet, utilizar recursos de RED entre otros.

- **Repositorio:** Almacén o lugar donde se guarda la información.

- **Unidad de red:** Es disco compartido en el que varios miembros de la red local usualmente denominado “grupo de trabajo” puede almacenar, tomar o compartir documentos o carpetas.

- **Carpeta:** Directorio especifico asignado para almacenar documentos.

- **Backups:** Se refiere a la copia de datos de Respaldo, de modo que se puedan utilizar para la restauración de la información original después de una eventual pérdida incluido el diferencial en los datos desde la última copia realizada.
- **Regla 3 2 1:** Realiza 3 copias de los datos en 2 soportes diferentes y alojar la tercera copia en 1 lugar físico distinto.

5. POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN

5.1 INSTALACIÓN DE SOFTWARE

Propósito: Minimizar el riesgo de exposición y de infección por malware, evitando a su vez posibles sanciones por el uso de software sin licenciar.

Política
Los trabajadores no deben instalar software en los dispositivos de la compañía sin la respectiva autorización del área de Tecnología. Las peticiones de instalación de software deben ser aprobadas por el administrador de la red y el proceso de instalación debe ser realizado por personal calificado de la compañía.
Todo software que sea instalado debe tener licenciamiento comercial o ser de licenciamiento libre (*Open Source* en Inglés). No se permite la instalación de software de propiedad particular; todo software que se utilice para el desarrollo de las actividades de negocio debe estar licenciado por la compañía.

5.2 USO DEL INTERNET EMPRESARIAL Y POLÍTICA DE MONITOREO

Propósito: El propósito de esta política es definir los estándares para el monitoreo y limitación de la navegación por Internet desde cualquier dispositivo en la red empresarial. Estos estándares están diseñados para asegurar que los empleados utilicen el Internet de forma segura y responsable.

Política
La Presidencia, o cualquiera de las Gerencias de las diferentes áreas, a través del Área de TI, están en potestad de monitorear el tráfico de red de todas las comunicaciones entrantes y salientes dentro de la red de la organización. Esto incluye conocer la IP de origen, la fecha, la hora, el protocolo, el servidor o dirección de destino.

La Presidencia, o cualquiera de las Gerencias de las diferentes áreas, pueden solicitar a través del Área de TI, el bloqueo de los sitios de Internet que se consideren inapropiados para el ambiente empresarial. Se considera una falta disciplinaria bajo cualquier circunstancia el acceso a páginas y sitios web de contenido sexual explícito, sitios de juegos o apuestas, sitios relacionados con sustancias ilícitas, sitios de citas, sitios de fraude, contenidos SPAM o en relación a delitos tipificados por la ley colombiana, contenido racista o de alguna forma ofensivo y discriminatorio, contenido violento, y todo contenido que no

esté relacionado con el desarrollo de las finalidades de la empresa sin que medie previa autorización.

Está totalmente prohibido el uso de la infraestructura empresarial para realizar ataques informáticos o similares.

Está restringido el uso del Internet en horas no autorizadas para acceder a contenido multimedia no asociado a la labor del empleado.

Cualquier intento por evadir los controles técnicos impuestos, será considerado en sí mismo una falta disciplinaria.

5.3 USO DE CORREO ELECTRÓNICO Y COMUNICACIONES PERSONALES

Propósito: Prevenir daños y perjuicios en la imagen o el nombre de la organización por el manejo incorrecto de los servicios de comunicación.

Política
Los diferentes medios de comunicación a disposición de los trabajadores no deben ser utilizados para la distribución de mensajes con contenido ofensivo, racista, discriminatorio, pornográfico, sexual, político, etc. Los empleados que reciban comunicaciones con este contenido deben eliminarlo inmediatamente y reportar el incidente si es de origen interno.

No está permitido utilizar los correos empresariales para la distribución de mensajes cadena, spam o de alguna forma comercial.

Los empleados no deben tener expectativa de privacidad alguna en el contenido que almacenen o envíen como parte de los servicios de comunicación de la compañía.

El no cumplimiento de las condiciones mencionadas anteriormente es considerado una falta disciplinaria y puede ser objeto de sanción.

Son deberes de los usuarios del servicio de correo electrónico corporativo:

- Informar a la brevedad al administrador del servicio cualquier supuesto incidente (mensajes en pantalla o anomalías en el servicio), debilidad, o violación de seguridad, de tal manera que se puedan ejecutar las actividades para la investigación y corrección de los incidentes.

- No divulgar información confidencial o secreta (conocida y utilizada por empleados de la empresa y/o algunas entidades externas autorizadas).

- No realizar pruebas para detectar y/o utilizar una supuesta debilidad o falla de seguridad.

- No enviar mensajes a través del correo electrónico con contenido que viole alguna patente, marca, secreto comercial, derecho de autor o cualquier derecho de propiedad de algún tercero.

- No incluir como destinatario/s de algún mensaje de correo electrónico, a todos aquellos que hayan manifestado su decisión de dejar de ser considerado/s como tal/es.

- No adjuntar en un mensaje de correo electrónico, aunque no sea enviado (almacenado en las carpetas), archivos/software que contengan virus informáticos, o que presenten sectores defectuosos, o de cualquier otro tipo de contenido que puedan provocar daño alguno.

5.4 MANEJO DE CLAVES

Propósito: El propósito de esta política es establecer un estándar de generación de contraseñas seguras, la protección de dichas contraseñas y su frecuencia de cambio.

Política
Para hacer uso de los recursos de tecnología a través de la red de datos, cada usuario debe utilizar un sistema de identificación única conformada por al menos dos datos que se llaman credenciales de usuario que son NOMBRE DE USUARIO y CONTRASEÑA; esta pareja de datos identifica de manera única y sin posibilidad de error a un único usuario y lo diferenciará de los demás usuarios. A través de la credencial de usuario el empleado podrá acceder a la información dispuesta para él según los privilegios y restricciones creados.

Las contraseñas no se deben escribir en lugares donde personas no autorizadas puedan descubrirlas. Aparte de la asignación inicial de la contraseña y del reajuste de la contraseña, si existe sospecha sobre la divulgación de una contraseña a alguien diferente del usuario autorizado, la contraseña debe ser cambiada inmediatamente.

Todas las contraseñas de nivel de Administrador, y otras que son usadas para diferentes procesos o software, se encuentran almacenadas a través del software KeePass, desde el cual se comparte con las personas adecuadas por medio de la cuenta de correo corporativa.

Todas las contraseñas de nivel de usuario (cuentas del dominio), deben ser cambiadas cada 2 meses, no pueden ser cambiadas por una contraseña usada ya anteriormente, y deben ser cambiadas teniendo en cuenta que no contenga el nombre o apellido, que no contengan caracteres de fácil recordación y deben contener mayúsculas, minúsculas y números; esta política está establecida desde el Directorio Activo para todas las cuentas de usuario.

Como base del correcto manejo de claves y contraseñas se presenta a continuación una serie de recomendaciones:

- Siempre utilice contraseñas diferentes para los servicios de la compañía y sus cuentas personales no relacionadas al ámbito laboral.
- No comparta sus contraseñas con ningún tercero, incluso si éste pertenece a la organización.
- Las contraseñas nunca deben estar escritas en texto plano (jamás archivos llamados claves.txt y en el escritorio).
- No revele las contraseñas por medios de comunicación desprotegidos como correo, mensajería instantánea, SMS, etc.
- Evite utilizar la opción de recordar contraseña en navegadores y programas internos.
- SI va a utilizar un computador que no es el propio, siempre navegue en el modo incógnito del browser.

5.5 REGISTRO DE ACTIVIDAD Y SUPERVISIÓN

Propósito: Registrar eventos y generar evidencia.

Política
Se producirán revisiones, en caso de ser necesario, a los registros de eventos que se graban de las actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

Los relojes de todos los sistemas de informática relevantes serán sincronizados a una fuente de tiempo de referencia única.

5.6 LA SEGURIDAD FÍSICA

Propósito: Evitar el acceso físico no autorizado, daños e interferencia para la información de la organización y las instalaciones de procesamiento de información.

Política
Los equipos de cómputo deben estar situados y protegidos para reducir los riesgos de las amenazas ambientales y los riesgos y las oportunidades de acceso no autorizado. El equipo deberá estar protegido contra fallas de energía y otras interrupciones causadas por fallas en el soporte de los servicios públicos. El cableado que transporta datos, energía y telecomunicaciones o el soporte de los servicios de información debe estar protegido contra la intercepción, interferencia o daños. Los equipos de cómputo deben tener un correcto mantenimiento para asegurar su continua disponibilidad e integridad.

Todos los elementos del equipo que contienen los medios de almacenamiento deberán ser verificados para garantizar que los datos sensibles y el software con licencia se han eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.

Los usuarios deberán asegurarse de que el equipo que no cuenta con vigilancia tenga la protección adecuada. Cuando un computador este desatendido deberá bloquearse la pantalla.

Los funcionarios deben procurar que el puesto de trabajo se mantenga libre de documentos y que los soportes de almacenamiento extraíbles estén en un lugar seguro.

5.7 REQUISITOS PARA EL CONTROL DE ACCESO A LOS CENTROS DE DATOS

Propósito: Limitar el acceso a las instalaciones y equipos de datos.

Política
Los trabajadores tienen la obligación de vigilar y garantizar que se cumplan las siguientes medidas de seguridad:

- El acceso a áreas seguras donde se procesa o almacena información confidencial y restringida es limitado únicamente a personas autorizadas.

- El acceso a áreas seguras requiere de esquemas de control de acceso, como tarjetas, llaves, candados, sistemas de registro facial o dactilar.

- Los empleados no deben acceder, manipular, abrir o modificar las conexiones de los Rack que puedan tener cerca a su puesto de trabajo, sin la debida autorización o supervisión del personal de TI.

- Se restringe el acceso físico a dispositivos como: puntos de acceso inalámbricos, *Routers*, *Gateways* y terminales de red que estén ubicadas en las áreas de trabajo.

5.8 ACCESO A DATOS SENSIBLES DE LOS EMPLEADOS

Propósito: Garantizar que los datos sensibles relacionados con los datos de la salud, creencias religiosas, políticas, sexuales, entre otros, de los trabajadores, solo puedan ser conocidos por el personal competente y pertinente en virtud de sus funciones, teniendo en cuenta el principio de Acceso Restringido.

Política
Las finalidades para las que son tratados los datos sensibles en la empresa, son limitadas y especificadas en las respectivas autorizaciones otorgadas por el titular de la información.

De forma general, el tratamiento de datos sensibles en la empresa, estará limitado únicamente a las divisiones de GESTIÓN HUMANA Y NÓMINA atendiendo las finalidades particulares autorizadas por el titular.

La empresa de forma particular y en los respectivos manuales de funciones según el cargo, determinará aquellos cargos particulares que podrán tener acceso a datos de carácter sensible, sin que ese acceso signifique una violación a la política de seguridad de acceso restringido.

Igualmente, aplican los mecanismos de seguridad identificados previamente como de acceso restringido a los datos personales.

5.9 CONFIDENCIALIDAD CON TERCEROS

Propósito: Establecer los requerimientos de confidencialidad en las relaciones con proveedores, contratistas, en particular con empleados y terceros en general.

Política
Para el desarrollo de las relaciones contractuales, comerciales y laborales, se debe exigir a los terceros la aceptación de los acuerdos de confidencialidad definidos por la organización. En dichos acuerdos se debe establecer el compromiso de salvaguardar la información, velar por su correcto uso, impedir el uso no autorizado de dicha información y guardar reserva. Se debe estipular a su vez la información que es objeto de protección dentro del acuerdo y su temporalidad.

Los acuerdos deben incluirse dentro de los contratos celebrados entre la organización y terceros, como parte integral del contrato a firmar como un acuerdo independiente.

La aceptación de las condiciones de confidencialidad es indispensable para conceder al tercero el acceso a la información protegida.

5.10 REVISIONES DE LA SEGURIDAD DE LA INFORMACIÓN

Propósito: Garantizar que la seguridad informática sea implementada y aplicada de acuerdo con las políticas y procedimientos de la organización.

Política
Los sistemas de información son revisados regularmente a través de Auditorías para cerciorarse que se da cumplimiento a las políticas y normas de seguridad de la información de la entidad.

5.11 RETENCION DE BACKUPS DE RETIRADOS

Propósito: Garantizar y definir el tiempo de retención de la información de los colaboradores una vez son retirados de la empresa.

Política

A todo empleado, que tenga cuenta de correo corporativa asignada, y por lo tanto equipo de cómputo a su cargo, una vez se notifica la cancelación, suspensión o retiro de la empresa, se procede a realizar un *backup* del correo corporativo, y de la información que se encuentra almacenada en el drive.

Dicha información es almacenada y retenida basándose en la siguiente política:

- El jefe directo debe informar si la persona va a ser reemplazada de manera inmediata, para que, en caso de ser así, se migre la información de la cuenta de la persona retirada a la activa.

- En caso de que no se tenga proyectado reemplazar a la persona, el jefe inmediato debe informar si dicha información se debe pasar a otro usuario, o por el contrario almacenada en el *Backup.*

- Los *Backups* serán almacenados y retenidos en la cuenta de Dropbox por un tiempo de 1 año; en caso de no recibir indicaciones de ser almacenado por mayor tiempo, se procederá a la eliminación definitiva.

6. PROCESO PARA LA ATENCIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

Toda vez que se presente algún incidente con la seguridad de la información tratada por AGROPECUARIA ALIAR S.A, deberá adelantarse el siguiente procedimiento:

1). **Reporte del Incidente de Seguridad Informática:** Ocurrido el Incidente de seguridad, la primera persona que tenga conocimiento del mismo, deberá inmediatamente presentar un reporte dirigido al área o persona encargada de la seguridad de la información, Área de TI, así como en el menor tiempo posible presentar un informe detallado sobre los hechos que del mismo se conocen.

2). **Reunión del comité de Seguridad de la información:** El área o persona encargada de la seguridad de la información, (Área de TI) convocará de forma extraordinaria la reunión de Comité de TI para la seguridad de la información, en el cual se desarrollarán los siguientes ítems.

   a. **Emisión del concepto técnico:** Evaluados los hechos del caso se deberá dar un concepto técnico que determina todas las contingencias surgidas en el caso en concreto.

   b. **Identificación de la falencia:** Como resultado del concepto técnico, se deberá identificar plenamente la falencia que dio pasó al Incidente de seguridad de la información.

   c. **Toma de Medidas:** El comité deberá tomar las medidas y los correctivos necesarios para evitar futuros Incidentes.

7. MODIFICACIÓN DE LAS POLÍTICAS

AGROPECUARIA ALIAR S.A se reserva el derecho de modificar la presente Política de Seguridad de la información en cualquier momento, comunicando de forma oportuna a todas aquellas personas que estén relacionadas o que participen en la manipulación de la información de la empresa para su correcta implementación.

8. CONTROL DE CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN
01/06/2021	01	Emisión del documento