Tipo de Documento: MANUAL DE POLITICAS Y ESTANDARES EN SEGURIDAD INFORMATICA	**Pertenece a:** DEPARTAMENTO DE SISTEMAS		**Fecha Elaboración** AGOSTO 20 DE 2014
Proceso :			**Fecha de Revisión** SEPTIEMBRE 19 DE 2014
Elaborado por: JORGE RAMOS	**Aprobado por:** JORGE RAMOS	**Autorizado por:** JORGE RAMOS	**No. Revisión** 1
Código y Título: MGA-001 MANUAL DE POLITICAS Y ESTANDARES EN SEGURIDAD INFORMATICA			

MANUAL DE POLITICAS Y ESTANDARES EN SEGURIDAD INFORMATICA

INTRODUCCION

Con la definición de las políticas y estándares de seguridad informática se busca establecer en el interior de la Organización una cultura de calidad con la operación en forma confiable.

La seguridad informática, es un proceso donde se deben evaluar y administrar los riesgos apoyados en políticas y estándares que cubran las necesidades de Avícola Triple A en materia de seguridad.

1. Desarrollo General

1.1Aplicación

Las políticas y estándares de seguridad informática tienen por objeto establecer medidas y patrones técnicos de administración y organización de las Tecnologías de Información y Comunicaciones TIC´s de todo el personal comprometido en el uso de los servicios informáticos proporcionados por el Área de Sistemas de Avícola Triple A S.A.S.

También se convierte en una herramienta de difusión sobre las políticas y estándares de seguridad informática a todo el personal de Avícola Triple A S.A.S. Facilitando una mayor integridad, confidencialidad y confiabilidad de la información generada por el Departamento de Sistemas, al personal, al manejo de los datos, al uso de los bienes informáticos tanto de hardware como de software disponible, minimizando los riesgos en el uso de las tecnologías de información.

1.2Evaluación de las Políticas

Las políticas tendrán una revisión periódica se recomienda que sea semestral para realizar actualizaciones, modificaciones y ajustes basados en las recomendaciones y sugerencias.

1.3Beneficios

Las políticas y estándares de seguridad informática establecidas en el presente documento son la base fundamental para la protección de los activos informáticos y de toda la información del Departamento de Sistemas en la Organización.

2 Seguridad Organizacional

Política: Toda persona que ingresa como usuario nuevo a Avícola Triple A S.A.S. para manejar equipos de cómputo y hacer uso de servicios informáticos debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar al pie de la letra las directrices impartidas en el Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

2.1Usuarios Nuevos

Todo el personal nuevo de la Organización, deberá ser notificado al Departamento de Sistemas, para asignarle los derechos correspondientes (Equipo de Cómputo, Creación de Usuario para la Red, Perfil para el ingreso a los aplicativos de la Organización) o en caso de retiro del funcionario, anular y cancelar los derechos otorgados como usuario informático.

2.2Obligaciones de los usuarios

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática para Usuarios del presente Manual.

2.3Capacitación en seguridad informática

Todo servidor o funcionario nuevo en Avícola Triple A S.A.S. deberá contar con la inducción sobre las Políticas y Estándares de Seguridad Informática Manual de Usuarios, donde se den a conocer las obligaciones para los usuarios y las sanciones en que pueden incurrir en caso de incumplimiento.

2.4 Sanciones

Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial de esta dependencia, o de que se le declare culpable de un delito informático.

3.- Seguridad física y del Medio Ambiente

Política: Para el acceso a los sitios y áreas restringidas se debe notificar al Departamento de Sistemas para la autorización correspondiente, y así proteger la información y los bienes informáticos.

3.1 Protección de la información y de los bienes informáticos

3.1.1 El usuario o funcionario deberán reportar de forma inmediata al Departamento de Sistemas cuando se detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio.

3.1.2 El usuario o funcionario tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante

3.1.3 Es responsabilidad del usuario o funcionario evitar en todo momento la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

3.2Controles de acceso físico

3.2.1 Cualquier persona que tenga acceso a las instalaciones Avícola Triple A S.A.S., deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la entidad, en el área de recepción o portería, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente.

3.2.2 Las computadoras personales, las computadoras portátiles, y cualquier activo de tecnología de información, podrá ser retirado de las instalaciones de Avícola Triple A S.A.S. únicamente con la autorización de salida del Departamento de Sistemas, anexando el comunicado de autorización del equipo debidamente firmado por un funcionario de Auditoría y por el Jefe de Sistemas.

3.3Seguridad en áreas de trabajo

Los Centros de Cómputo de Avícola Triple A S.A.S. son áreas restringidas, por lo que solo el personal autorizado por el Departamento de Sistemas puede acceder a él.

3.4Protección y ubicación de los equipos

3.4.1 Los usuarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del Departamento de Sistemas, en caso de requerir este servicio deberá solicitarlo.

3.4.2 El Área Financiera que tiene el control de Inventarios de activos será la encargada de registrar en el sistema de Activos Fijos el responsable de los activos informáticos que le asignen.

3.4.3 El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones de los funcionarios o servidores de Avícola Triple A S.A.S.

3.4.4 Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

3.4.5 Es responsabilidad de los usuarios almacenar su información únicamente en la carpeta de trabajo indicada por el Departamento de Sistemas.

3.4.6 Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.

3.4.7 Se debe evitar colocar objetos encima del equipo cómputo o tapar las salidas de ventilación de los equipos de cómputo como portátiles, video proyectores, CPU de equipos de escritorio, monitores, estabilizadores y UPS.

3.4.8 Se debe mantener el equipo informático en un lugar limpio y sin humedad.

3.4.9 El usuario debe asegurarse que los cables de conexión no sean pisados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar un reubicación de cables con el personal del Departamento de Sistemas.

3.4.10 Cuando se requiera realizar cambios múltiples de los equipo de cómputo derivado de reubicación de lugares físicos de trabajo o cambios locativos, éstos deberán ser notificados con tres días de anticipación al Departamento de Sistemas mediante correo electrónico con un detallado.

3.4.11 Queda terminantemente prohibido que el usuario o funcionario distinto al personal del Departamento de Sistemas abra o destape los equipos de cómputo.

3.4.12 Los equipos portátiles deben estar siempre protegidos por su guaya de seguridad, en caso de encontrarse en las rondas de seguridad sin presencia del usuario asignado y sin protección de la guaya de seguridad el personal de seguridad lo llevara a sitio seguro donde el usuario lo podrá reclamar.

3.5Mantenimiento de equipos

3.5.1 Únicamente el personal autorizado por el Departamento de Sistemas podrá llevar a cabo los servicios y reparaciones al equipo informático.

3.5.2 Los usuarios deberán asegurarse de respaldar en copias de respaldo o Backups la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo,

previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

3.6Pérdida de Equipo

3.6.1 El servidor o funcionario que tengan bajo su responsabilidad o asignados algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

3.6.2 El préstamo de video proyectores, laptops o portátiles tendrá que solicitarse al Departamento de Sistemas, con registro el evento en el formato de préstamo de equipos.

3.6.3 El servidor o funcionario deberán dar aviso inmediato al Departamento de Sistemas, y a la Administración de Inventarios de Activos de la desaparición, robo o extravío de equipos de cómputo, periféricos o accesorios bajo su responsabilidad.

3.7Uso de dispositivos extraíbles

3.7.1 El Departamento de Sistemas de Avícola Triple A S.A.S., velará porque todos los usuarios de los sistemas de Información estén registrados en su Base de Datos para la autorización de uso de equipos portátiles, dispositivos de almacenamiento externo, como Pen Drives o Memorias USB, Discos portátiles, Unidades de Cd y DVD Externos, para el manejo y traslado de información o realización de copias de seguridad o Backups.

3.7.2 Cada Jefe de Área o dependencia debe reportar al Departamento de Sistemas el listado de funcionarios a su cargo que manejan estos tipos de dispositivos, especificando clase, tipo y uso determinado.

3.7.1 El uso de los quemadores externos o grabadores de disco compacto es exclusivo para Backups o copias de seguridad de software y para respaldos de información que por su volumen así lo justifiquen.

3.7.2 El servidor o funcionario usuario que tengan asignados estos tipos de dispositivos serán responsable del buen uso de ellos.

3.7.3 Si algún área o dependencia por requerimientos muy específicos del tipo de aplicación o servicios de información tengan la necesidad de contar con uno de ellos, deberá ser justificado y autorizado por la Gerencia General.

3.7.4 Todo funcionario o servidor de Avícola Triple A S.A.S. deberá reportar al Departamento de Sistemas el uso de las memorias USB asignados para su trabajo y de carácter personal y responsabilizarse por el buen uso de ellas.

3.8 Daño del equipo

3.8.1 El equipo de cómputo, periférico o accesorio de tecnología de información que sufra algún desperfecto, daño por maltrato, descuido o negligencia por parte del usuario responsable, se le levantara un reporte de incumplimiento de políticas de seguridad.

4. Administración de Operaciones en los Centros de Cómputo

Política: Los usuarios y funcionarios deberán proteger la información utilizada en la infraestructura tecnológica de Avícola Triple A S.A.S. De igual forma, deberán proteger la información reservada o confidencial que por necesidades organizacionales deba ser guardada, almacenada o transmitida, ya sea dentro de la red interna organizacional a otras dependencias de sedes alternas o redes externas como internet.

4.1.1 Los usuarios y funcionarios de Avícola Triple A S.A.S. que hagan uso de equipos de cómputos, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, caballos de Troya o gusanos de red.

4.1.2 El Departamento de Sistemas en cabeza del Jefe de Sistemas con el apoyo de Gerente Corporativo de Sistemas, establece las políticas y procedimientos administrativos para regular, controlar y describir el acceso de visitantes o funcionarios no autorizados a las instalaciones de cómputo restringidas.

4.1.3. El Centro de Cómputo debe estar en un recinto cerrado bajo llave que cuente con las condiciones eléctricas, climáticas, y de iluminación adecuadas para que los equipos se mantengan a una temperatura de 21 a 23 grados centígrados y protegidos de riesgos de acceso.

4.1.4 Cuando un funcionario no autorizado o un visitante requieran la necesidad de ingresar a la Sala donde se encuentren los Servidores, debe solicitar mediante comunicado interno debidamente firmada y autorizado por el Jefe inmediato de su sección o dependencia y para un visitante se debe solicitar la visita con anticipación la cual debe traer el visto bueno de la Gerencia General, y donde se especifique tipo de actividad a realizar, y siempre contar con la presencia de un funcionario del Departamento de Sistemas.

4.1.5 El Jefe de Sistemas deberá llevar un registro escrito de todas las visitas autorizadas a los Centros de Cómputo restringidos.

4.1.6 Todo equipo informático ingresado a los Centros de Cómputo restringidos deberá ser registrado en el libro de visitas.

4.1.7 Cuando se vaya a realizar un mantenimiento en algunos de los equipos del Centro de Cómputo restringido, se debe dar aviso con anticipación a los usuarios para evitar traumatismos.

4.1.8 El Jefe de Sistemas deberá solicitar a la Gerencia General los equipos de protección para las instalaciones contra incendios, inundaciones, sistema eléctrico de respaldo, UPS.

4.2Uso de medios de almacenamiento

4.2.1 Los usuarios y servidores de Avícola Triple A deben conservar los registros o la información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial.

4.2.2 Las actividades que realicen los usuarios y funcionarios en la infraestructura de los Sistemas de Avícola Triple A S.A.S. serán registradas y podrán ser objeto de auditoría.

4.3Adquisición de software.

4.3.1 Los usuarios y funcionarios que requieran la instalación de software que o sea propiedad de Avícola Triple A, deberán justificar su uso y solicitar su autorización por el Departamento de Sistemas con el visto bueno de su Jefe inmediato, indicando el equipo de cómputo donde se instalará el software y el período de tiempo que será usado.

4.3.2 Se considera una falta grave el que los usuarios o funcionarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de Avícola Triple A S.A.S., que no esté autorizado por el Departamento de Sistemas.

4.3.3 El Departamento de Sistemas, tiene a su cargo la tarea de informar periódicamente a la comunidad, Directivos, Administrativos, usuarios de sistemas su política organizacional contra la piratería de software, utilizando todos los medios de comunicación disponibles: Página WEB, Emails, Carteleras y Boletines. Debemos considerar también la publicación de las posibles sanciones o multas en los que se puede incurrir.

4.3.4 Avícola Triple A S.A.S. tiene cien por ciento Licenciado el Software que es utilizado en toda su Infraestructura de Sistemas. Cualquier "software" requerido será adquirido a sus Proveedores debe ser debidamente certificado, el cual deberá entregar al momento de la compra, el programa y la licencia del software con toda la documentación pertinente y necesaria que certifique la originalidad y validez del mismo.

4.3.5 El control de manejo para las licencias y el inventario de los Medios, paquete de CD´s será responsabilidad del Departamento de Sistemas en cabeza del Jefe de Sistemas, o su delegado, en caso de ausencia.

4.3.6 El Departamento de Sistemas tiene la responsabilidad de velar por el buen uso de los equipos de cómputo y del cumplimiento de las políticas de seguridad. A

su vez deberán ofrecer mantenimiento preventivo a las computadoras de la Organización.

4.3.7 En el proceso de reinstalar un programa el técnico debe borrar completamente la versión instalada para luego proceder a instalar la nueva versión que desea, esto siempre y cuando no sea una actualización del mismo.

4.3.8 Deben mantener un inventario de equipos físicos y de los programas instalados y pueden borrar o instalar programas o software autorizados y legalmente licenciados. Cualquier otra petición de software deberá ser tramitada a través del Departamento de Sistemas, utilizando el correo electrónico. Las Licencias se almacenan en la carpeta

Finalmente se procede a actualizar el inventario de licencias de Software cuyo contrato tiene una vigencia anual. Y se almacenará en Archivos que puedan ser cerrados con llave.

4.4 Licenciamiento de Software

4.4.1 Para el Control de Licenciamiento de Software: Avícola Triple A S.A.S. al realizar la compra de los equipos de cómputo de una vez se adquieren las licencias de software que sean necesarias para su funcionamiento, si se requiere algún software adicional debe ser tramitado por el Departamento de Sistemas, además como política de seguridad se tiene establecido la prohibición de instalar software y programas no autorizados y sin licencia. El Departamento de Sistemas realiza periódicamente un inventario físico de los programas y software instalados en cada uno de los computadores de la organización.

4.5Identificación del incidente

4.5.1 El usuario o funcionario que detecte o tenga conocimiento de la posible ocurrencia de un incidente de seguridad informática deberá reportarlo al Departamento de Sistemas lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

4.5.2 Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las Directivas Administrativas competentes, el usuario o funcionario informático deberá notificar al Departamento de Sistemas.

4.5.3 Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información de Avícola Triple A S.A.S. debe ser reportado al Departamento de Sistemas.

4.6Administración de la Red

4.6.1 Los usuarios de Avícola Triple A no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la entidad, sin la autorización del Departamento de Sistemas.

4.7Seguridad para la red

4.7.1 Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por el Departamento de Sistemas, en la cual los usuarios o funcionarios realicen la exploración de los recursos informáticos en la red de Avicola Triple A S.A.S., así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

4.8 Uso del Correo electrónico

4.8.1 Los usuarios y funcionarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe redireccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa Avícola Triple A S.A.S., a menos que cuente con la autorización del Departamento de Sistemas.

4.8.2 Los usuarios y funcionarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad de Avícola Triple A S.A.S. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

4.8.3 Queda prohibido falsificar, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

4.8.4 Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

4.9 Controles contra virus o software malicioso

4.9.1 Para revisar si el antivirus se actualiza correctamente, seleccione el icono de su programa antivirus KasperSky y coloque el ratón sobre este ícono, aparecerá un mensaje con las fechas de actualización del antivirus o las advertencias a que tenga lugar, en cuyo caso dará la opción de actualizar o corregir el problema.

Puede que este proceso ponga un poco más lenta a la máquina, pero por ningún motivo interrumpa la actualización. Una vez terminada la actualización el programa le indicará que la base de firmas queda actualizada. El servidor de seguridad está ubicado dentro de la red así que no genera tráfico hacia internet.

4.9.2 Para prevenir infecciones por virus informático, los usuarios de Avícola Triple A S.A.S. no deben hacer uso de software que no haya sido proporcionado y validado por el Departamento de Sistemas.

4.9.3 Los usuarios de Avícola Triple A S.A.S. deben verificar que la información y los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por el Departamento de Sistemas.

4.9.4 Todos los archivos de computadoras que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el usuario debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse.

4.9.5 Ningún usuario, funcionario, empleado o personal externo, podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización del Departamento de Sistemas.

4.9.6 Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y notificar al Departamento de Sistemas para la revisión y erradicación del virus.

El icono del antivirus KasperSky debe permanecer siempre con fondo blanco, si usted observa dicho icono en otro color, favor avisar inmediatamente al Departamento de Sistemas, para que se haga la revisión correspondiente.

4.9.7 Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por el Departamento de Sistemas en: Antivirus, Herramientas Office, Navegadores u otros programas.

4.9.8 Debido a que algunos virus son extremadamente complejos, ningún usuario o funcionario de Avícola Triple A S.A.S., distinto al personal del Departamento de Sistemas deberá intentar erradicarlos de las computadoras.

4.10 Controles para la Generación y Restauración de Copias de Respaldo (Backups)

4.10.1 Procedimiento de generación y restauración de copias de respaldo para salvaguardar la información crítica de los procesos significativos de la entidad. Se deberán considerar como mínimo los siguientes aspectos:

4.10.1.1 Establecer como medida de seguridad informática la necesidad de realizar copias de respaldo o backups periódicamente en los equipos de cómputo administrativos y servidores.

4.10.1.2 Cada funcionario es responsable directo de la generación de los backups o copias de respaldo, asegurándose de validar la copia. Este proceso corre automáticamente en su equipo También puede solicitar asistencia técnica para la restauración de un backups.

4.10.1.3 Conocer y manejar el software utilizado para la generación y/o restauración de copias de respaldo, registrando el contenido y su prioridad. Rotación de las copias de respaldo, debidamente marcadas.

4.10.1.4 Las copias de seguridad o Back ups se deben realizar al menos una vez a la semana y el último día hábil del mes. Un funcionario del Departamento de Sistemas, revisará una vez por semana, el cumplimiento de este procedimiento y registrará en el formato de Copias de Seguridad.

4.11 Planes de Contingencia ante Desastre

Definición: Se entiende por PLAN DE CONTINGENCIA los procedimientos alternativos a la operación normal en una organización, cuyo objetivo principal es permitir el continuo funcionamiento y desarrollo normal de sus operaciones, preparándose para superar cualquier eventualidad ante accidentes de origen interno o externo, que ocasionen pérdidas importantes de información. Estos deben prepararse de cara a futuros sucesos.

4.11.1 Con el fin de asegurar, recuperar o restablecer la disponibilidad de las aplicaciones que soportan los procesos de misión crítica y las operaciones informáticas que soportan los servicios críticos de la organización, ante el evento de un incidente o catástrofe parcial y/o total.

4.11.2 El Departamento de Sistemas debe tener en existencia la documentación de roles detallados y tareas para cada una de las personas involucradas en la ejecución del plan de recuperación ante desastre.

4.11.3 Disponibilidad de plataformas computacionales, comunicaciones e información, necesarias para soportar las operaciones definidas como de misión crítica de negocio en los tiempos esperados y acordados.

4.11.4 Tener en existencia equipos informáticos de respaldo o evidencia de los proveedores, de la disponibilidad de equipos y tiempos necesarios para su instalación, en préstamo, arriendo o sustitución.

4.11.5 Existencia de documentación de los procedimientos manuales a seguir por las distintas áreas usuarias durante el periodo de la contingencia y entrenamiento a los usuarios en estos procedimientos.

4.11.6 Existencia de documentación de los procedimientos detallados para restaurar equipos, aplicativos, sistemas operativos, bases de datos, archivos de información, entre otros.

4.11.7 Existencia de documentación de pruebas periódicas de la implementación del plan de recuperación ante desastre para verificar tiempos de respuesta, capitalizando los resultados de la pruebas para el afinamiento del plan.

4.11.8 Actualización periódica del plan de recuperación ante desastre de acuerdo con los cambios en plataformas tecnológicas (hardware, software y comunicaciones), para reflejar permanentemente la realidad operativa y tecnológica de la compañía.

4.11.9 Disponibilidad de copias de respaldo para restablecer las operaciones en las áreas de misión crítica definidas.

4.12 Internet

4.12.1 El acceso a Internet provisto a los usuarios y funcionarios de Avícola Triple A S.A.S. es exclusivamente para las actividades relacionadas con las necesidades del cargo y funciones desempeñadas.

4.12.2 Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por Avícola Triple A S.A.S. en caso de necesitar una conexión a Internet alterna o especial, ésta debe ser notificada y aprobada por el Departamento de Sistemas.

4.12.3 Los usuarios de Internet de Avícola Triple A S.A.S. tienen que reportar todos los incidentes de seguridad informática al Departamento de Sistemas inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

4.12.4 Los usuarios del servicio de navegación en Internet, al aceptar el servicio están aceptando que:

 Serán sujetos de monitoreo de las actividades que realiza en Internet, saben que existe la prohibición al acceso de páginas no autorizadas, saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.

Saben que existe la prohibición de descarga de software sin la autorización del Departamento de Sistemas.

 La utilización de Internet es para el desempeño de sus funciones y cargo en Avícola Triple A S.A.S. y no para propósitos personales.

5. Acceso Lógico

Política: Cada usuario y funcionario son responsables de los mecanismos de control de acceso que les sean proporcionados; esto es, de su “ID” login de usuario y contraseña necesarios para acceder a la red interna de información y a la infraestructura tecnológica de Avícola Triple A S.A.S., por lo que se deberá mantener de forma confidencial.

El permiso de acceso a la información que se encuentra en la infraestructura tecnológica de Avícola Triple A S.A.S. , debe ser proporcionado por el dueño de la información, con base en el principio de “Derechos de Autor” el cual establece que únicamente se deberán otorgar los permisos mínimos necesarios para el desempeño de sus funciones.

5.1 Controles de acceso lógico

5.1.1 Todos los usuarios de servicios de información son responsables por el de usuario y contraseña que recibe para el uso y acceso de los recursos.

5.1.2 Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por el Departamento de Sistmeas antes de poder usar la infraestructura tecnológica de Avícola Triple A S.A.S.

5.1.3 Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de Avícola Triple A S.A.S., a menos que se tenga el visto bueno del dueño de la información y del Departamento de Sistemas y la autorización del Gerente General o de su Jefe inmediato.

5.1.4 Cada usuario que acceda a la infraestructura tecnológica de Avícola Triple A S.A.S debe contar con un identificador de usuario (ID) único y personalizado. Por lo cual no está permitido el uso de un mismo ID por varios usuarios.

5.1.5 Los usuarios y funcionarios son responsables de todas las actividades realizadas con su identificador de usuario (ID). Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, al igual que tiene prohibido utilizar el ID de otros usuario.

5.2 Administración de privilegios

5.2.1 Cualquier cambio en los roles y responsabilidades de los usuarios deberán ser notificados al Departamento de Sistemas, para el cambio de privilegios, Ver Manual de Roles.

5.3 Equipo desatendido

5.3.1 Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla (screensaver) previamente

instalados y autorizados por el Departamento de Sistemas cuando no se encuentren en su lugar de trabajo.

5.4 Administración y uso de contraseñas

5.4.1 La asignación de contraseñas debe ser realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido, como política el sistema exige que tengan una longitud mínima de 7 caracteres, exige historial de 24 contraseñas recordadas, debe cumplir con los requisitos de complejidad y tiene validez de 30 días.

5.4.2 Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá acudir al Departamento de Sistemas para que se le proporcione una nueva contraseña.

5.4.3 Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos.

5.4.4 Sin importar las circunstancias, las contraseñas nunca se deben compartir o revelar. Hacer esto responsabiliza al usuario que prestó su contraseña de todas las acciones que se realicen con el mismo.

5.4.5 Todo usuario que tenga la sospecha de que su contraseña es conocido por otra persona, deberá cambiarlo inmediatamente.

5.4.6 Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

5.5 Controles para Otorgar, Modificar y Retirar Accesos a Usuarios

5.5.1 Cualquier nuevo rol creado por el Departamento de Sistemas se deberá analizar y concertar con el Jefe de Recursos Humanos y el Jefe de Contabilidad.

5.5.2 Todo usuario debe quedar registrado en la Base de Datos Usuarios y Roles.

La creación de un nuevo usuario y/o solicitud para la asignación de otros roles dentro del sistema de Avícola Triple A S.A.S .deberá de venir acompañado del correo del Departamento de Recursos Humanos quien informa el ingreso del funcionario (para la creación en el Directorio Activo y el servidor de correo) si es necesario el ingreso a la ERP se requiere la autorización del Jefe de Contabilidad, para el ingreso al Sistema de Nómina o al PortalMU se requiere la autorización del Jefe de Recursos Humanos.

5.5.3 El Departamento de Sistemas, en cabeza del Jefe de Sistemas o su delegado en caso de ausencia, será la responsable de ejecutar los movimientos de altas, bajas o cambios de perfil de los usuarios.

5.6 Control de accesos remotos

5.5.1 La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con el visto bueno y con un mecanismo de control de acceso seguro autorizado por el dueño de la información y del Departamento de Sistemas.

6. Cumplimiento de Seguridad Informática

Política: El Departamento de Sistmeas tiene como una de sus funciones la de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de bancos de datos de información automatizada en general.

7. Derechos de propiedad intelectual

7.1 Los sistemas desarrollados por personal interno o externo que controle el Departamento de Sistemas son propiedad intelectual de Avícola Triple A S.A.S.

8. Cláusulas de cumplimiento

8.1 El Departamento de Sistemas realizará acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática.

8.2 El Departamento de Sistemas podrá implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado en la política de Seguridad de Personal.

8.3 Los jefes y responsables de los procesos establecidos en Avícola Triple A S.A.S. deben apoyar las revisiones del cumplimiento de los sistemas con las políticas y estándares de seguridad informática apropiadas y cualquier otro requerimiento de seguridad.

9 Violaciones de seguridad Informática

9.1 Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por el Departamento de Sistemas.

9.2 Ningún usuario o funcionario de Avícola Triple A S.A.S. debe probar o intentar probar fallas de la Seguridad Informática conocidas, a menos que estas pruebas sean controladas y aprobadas por el Departamento de Sistemas.

9.3 No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, diseñado para auto

replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información de Avícola Triple A S.A.S.

10. Equipos en el Área Administrativa

10.1 Avícola Triple A S.A.S. deberá poner a disposición del Departamento de Sistemas, la información contractual de los equipos informáticos de Cómputo Escritorio, Portátil y periférica, así como de los servicios de soporte y mantenimiento.

10.2 El Departamento de Sistemas, será quien valide el cumplimiento de las Condiciones Técnicas de los equipos informáticos de Cómputo Escritorio, Portátiles y Periféricos adquiridos.

10.3 El Departamento de Sistemas, tendrá bajo su resguardo las licencias de software, los medios de Instalación y manuales, para llevar los controles de software instalado, para los equipos informáticos de cómputo Escritorio, Portátiles y periféricos al momento de la recepción de los mismos.

10.4 Los requerimientos de Equipos Informáticos de Cómputo Escritorio, Portátiles y periféricos, se llevarán a cabo mediante la solicitud y justificación por escrito, firmada por el Jefe del Área solicitante, lo cuales serán evaluados por el Departamento de Sistemas para su autorización e inclusión en el Presupuesto correspondiente.

10.5 El Departamento de Sistemas, es el área encargada de tramitar las asignaciones, reasignaciones, bajas, etc. de equipos informáticos de cómputo Escritorio, Portátiles y periféricos ante la Sección Financiera entidad encargada del Inventario de Activos para su ejecución, con base a las solicitudes realizadas al respecto y las revisiones de aprovechamiento de los mismos.

10.6 El Departamento de Sistemas, llevara el registro en cada asignación o movimiento de equipos informáticos de cómputo Escritorio, Portátiles y periféricos, el cual contiene los datos generales del usuario y de los bienes informáticos entregados, así mismo, contendrá los datos de software instalado autorizado y configuración del equipo, contando con la firma de conformidad del usuario correspondiente.

10.7 Queda prohibido a los usuarios mover los equipos informáticos de cómputo Escritorio, Portátiles y periféricos por su propia cuenta, el usuario deberá solicitar al Departamento de Sistemas el movimiento así como informar la razón del cambio y en su caso, requerir la reasignación del equipo.

10.8 El Departamento de Sistemas deberá elaborar el documento de salida cuando algún bien informático de cómputo Escritorio, Portátiles y periférico

requiera ser trasladado fuera de las instalaciones de Avícola Triple A S.A.S. por motivo de garantía, reparación o evento.

10.9 Si algún equipo informático de cómputo Escritorio, Portátiles o periférico es trasladado por el usuario a oficinas distintas al lugar asignado, oficinas externas o foráneas para realizar sus labores, dicho bien estará bajo resguardo del responsable que retira el equipo y el documento de salida quedará a consideración del Departamento de Sistemas para su autorización y visto bueno.

10.10 Las diferentes Áreas de Avícola Triple A S.A.S serán encargadas de proporcionar al Departamento de Sistemas, la relación de bienes y equipos que entrarán al proceso de baja, según corresponda. El Departamento de Sistemas realizara la evaluación técnica del equipo y definirá la reasignación o baja definitiva del bien que será informada a Área Financiera para control de Inventarios de Activos por medio del procedimiento definido por el mismo.

10.11 Queda prohibida la baja de equipo de cómputo que no cuente con evaluación técnica por parte del Departamento de Sistemas.

10.12 El Departamento de Sistemas no es responsable de proporcionar asesoría técnica, mantenimiento preventivo o correctivo a equipo de cómputo propiedad del usuario.

10.13 El usuario que ingrese equipos de su propiedad a las instalaciones de Avícola Triple A S.A.S. es responsable de la información almacenada en el mismo, y deberá mantener la privacidad, integridad y respaldos de la misma sin ser esto responsabilidad del Departamento de Sistemas.

10.14 Queda prohibido instalar software no autorizado o que no cuente con licencia, el Departamento de Sistemas deberá realizar las instalaciones de acuerdo con los estándares de Avícola Triple A S.A.S.

10.15 Es responsabilidad del usuario a quien esté asignado el equipo de escritorio o portátil, la información contenida en la misma.

10.16 Cuando un usuario cambie de área, el equipo asignado a éste deberá permanecer dentro del área designada originalmente. Será responsabilidad de la nueva área en la que habrá de laborar el usuario, el proporcionarle equipo de cómputo para el desarrollo de sus funciones.

10.17 En el caso de reinstalaciones de equipo, el usuario será el responsable de verificar que toda la información y archivos de trabajo estén contenidos en el equipo asignado, el usuario deberá firmar la Solicitud proporcionado por el técnico o ingeniero asignado firmando de conformidad.

10.18 El Departamento de Sistemas no es responsable de la configuración de dispositivos personales tales como Tabletas, Palms, iPOD y teléfonos celulares propiedad del usuario.

10.19 El usuario que requiera la instalación de Software de su propiedad deberá solicitar por escrito al Departamento de Sistemas anexando copia de la licencia que compruebe su propiedad o en el caso de software libre el documento probatorio.

10.20 Los equipos de cómputo adquiridos por Avícola Triple A S.A.S. se compran de una vez con su Licencia de Windows y la Suite de Microsoft Office, con esto garantizamos desde el principio su licenciamiento.