SECRETARÍA DE ESTADO

MINISTERIO DE AGRICULTURA Y GANADERÍA
GOBIERNO DE
EL SALVADOR
UNÁMONOS PARA CRECER

Santa Tecla, 1 de abril de 2016

Señor(a)
Jefe División de Informática
Presente

MINISTERIO DE AGRICULTURA Y GANADERÍA
ASUNTO: Políticas Informáticas del MAG.

HOY SE HA EMITIDO EL ACUERDO QUE DICE:

"ACUERDO Nº 171. Santa Tecla, 1 de abril de 2016. El Órgano Ejecutivo en el Ramo de Agricultura y Ganadería,

CONSIDERANDO:

I. Que por Decreto N° 4 de fecha 14 de septiembre de 2004, se emitieron las Nuevas Normas Técnicas de Control Interno de la Corte de Cuentas de la República.

II. Que por Decreto N° 09 de fecha 08 de febrero de 2013, se emitió el Reglamento de Normas Técnicas de Control Interno Específicas del Ministerio de Agricultura y Ganadería.

III. Que por Decreto N° 24 de fecha 24 de junio de 2014, se emitió el Reglamento para el Uso y Control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público.

IV. Que la gestión informática requiere de un instrumento administrativo que dicte las actuaciones del personal en cuanto al uso de los recursos informáticos; así como de lineamientos que apoye la toma de decisiones para las inversiones y control interno de los recursos informáticos del Ministerio.

POR TANTO,

En uso de sus facultades legales y a los considerandos que anteceden,

ACUERDA emitir las siguientes:

POLÍTICAS INFORMÁTICAS DEL MINISTERIO DE AGRICULTURA Y GANADERÍA

INTRODUCCION

Ante el esquema de globalización que las tecnologías de la información han originado principalmente por el uso masivo y universal de la Internet y sus tecnologías, las instituciones se ven inmersas en ambientes agresivos donde el delinquir, sabotear, robar se convierte en retos para delincuentes informáticos universales conocidos como Hackers, Crakers, etc., es decir en transgresores.

Conforme las tecnologías se desarrollan y adoptan, la severidad y frecuencia las van transformando en un continuo riesgo, que obliga a las entidades a crear medidas de emergencia y políticas definitivas para contrarrestar estos ataques y transgresiones.

La seguridad de las instituciones en muchos de los países se ha convertido en cuestión de seguridad nacional, por ello contar con un documento de políticas de seguridad es imprescindible, y debe de plasmar mecanismos confiables que con base en la política institucional proteja los activos de la Institución.

I. OBJETIVO

Establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes (Voz y Datos)) y personas que interactúan haciendo uso de los servicios asociados a ellos.

II. ALCANCE

La política de seguridad informática se aplica a todos los funcionarios y empleados del Ministerio de Agricultura y Ganadería.

III. DEFINICIONES

- MAG: Ministerio de Agricultura y Ganadería
- OGA: Oficina General de Administración.
- DBA: Administrador de la Base de Datos.
- La administración de Tecnología está integrada por el Director de la Oficina General de Administración, el Jefe de la División de Informática y los Coordinadores de las Áreas de Infraestructura informática, Desarrollo de sistemas de información y Soporte Técnico.
- Contraseña: Conjunto de caracteres que permite el acceso de un usuario a un recurso informático (password).
- DataCenter (Centro de Datos): Oficina con equipos de cómputo, telecomunicaciones y servidores que prestan servicios a todas las oficinas y dependencias del MAG, con las características físicas y ambientales adecuadas para que los equipos alojados funciones sin problema.
- Red: Equipos de cómputo, sistemas de información y redes de telemática del ministerio.
- Solución de Antivirus: Recurso informático empleado para solucionar problemas causados por virus informáticos.
- Usuario: Cualquier persona (empleado o no) que haga uso de los servicios de las tecnologías de información proporcionadas por el MAG, tales como equipos de cómputo, sistemas de información, redes de telemática.
- Virus informático: Programa ejecutable o pieza de código con habilidad de ejecutarse y reproducirse, regularmente escondido en documentos electrónicos, que causan problemas al ocupar espacio de almacenamiento, asi como destrucción de datos y reducción del desempeño de un equipo de cómputo.

IV. LINEAMIENTOS GENERALES

Planificación

4.1 La planificación informática se adecuará al sistema de planificación institucional; además, contará con los siguientes planes especiales:

a. Plan de seguridad, que tendrá la finalidad de proteger los recursos informáticos y la información institucional de daños o sustracción.
b. Plan de contingencia, para la pronta recuperación y restauración de los recursos y procesos informáticos ante emergencias, fallas o desastres.

4.2 La División de Informática del MAG emitirá anualmente estándares de especificaciones técnicas para la adquisición de:

a. Software comercial (sistemas operativos, aplicativos de oficina, antivirus, software de desarrollo, gestores y herramientas de base de datos).
b. Equipo informático y de comunicación.
c. Sistemas de información.

4.3 El software será clasificado de la siguiente forma:

a. Software básico: el sistema operativo, paquete de ofimática, antivirus
b. Paquetes utilitarios (software de diseño gráfico, especializado de audio y video, etc.)
c. Software para desarrollo de sistemas: el software básico y herramientas de usuario de desarrollo.

4.4 La División de Informática mantendrá un control de las licencias, asignación e instalación del software comercial y de los sistemas de información existentes. Con el objetivo de evaluar la continuidad o reemplazo del software, de acuerdo a las necesidades del MAG.

Sistema de información

4.5 El desarrollo de sistemas podrá hacerse tanto con recursos internos como a través de la contratación de servicios, previa evaluación de la conveniencia de la institución.

4.6 Para que la información obtenida a través de los sistemas automatizados sea confiable se considerará lo siguiente:

a. Los datos obtenidos a través de encuestas y estudios de campo, el control de calidad de los datos recolectados será realizados por un supervisor nombrado para este fin.
b. El control de calidad de los datos digitados en el sistema lo realizará personal diferente al que ingresó la información.
c. El control de calidad debe efectuarse por lo menos dos veces por semana cuando se realicen capturas masivas de datos y una vez cuando se trate del trabajo que el empleado realice a diario.
d. Los sistemas de información incluirán rutinas de validación y parametrización de datos (validación de fechas, cantidades y documentos de identificación entre otros). Los campos afectados serán definidos conjuntamente con el usuario.
e. Los sistemas de información contendrán reportes especiales para comprobar la consistencia de datos, los cuales serán definidos conjuntamente con las jefaturas beneficiarias del sistema y éstos podrán obtenerse de acuerdo a las necesidades de los interesados.
f. Las actualizaciones o cambios de datos, serán autorizadas por el jefe de la unidad o el director de la oficina beneficiaria.
g. El Administrador de la Base de Datos ejecutará planes de revisión de los datos almacenados, utilizando muestreos aleatorios. Además, definirá la selección de los sistemas de información, la frecuencia y el método que utilizará para realizar dicha labor.

4.7 La responsabilidad de la calidad de la información recae en los siguientes actores:

a. En la fase de ingreso de datos: la preparación de los documentos, la digitación, revisión de datos y salida de la información, el responsable directo es la oficina o unidad beneficiaria.
b. En el buen funcionamiento del sistema (procesamiento de datos) basado en los requerimientos solicitados por el usuario y el almacenamiento de la información el responsable es la División de Informática.

Adquisición de bienes informáticos

4.8 Toda adquisición de tecnología informática deberá contar con la aprobación de la División de Informática, así como al planear las operaciones relativas a la adquisición de bienes informáticos, se deberá establecer prioridades y tomando en cuenta:

a. Precio.
   Costo inicial, costo de mantenimiento y consumibles por el período estimado de uso de los equipos.
b. Calidad.
   Parámetro cualitativo que especifica las características técnicas de los recursos informáticos.
c. Experiencia
   Presencia en el mercado, estructura de servicio, la confiabilidad de los bienes y certificados de calidad con los que cuente.

d. Desarrollo tecnológico
   Se deberá analizar su grado de obsolescencia, su nivel tecnológico con respecto a la oferta existente y su permanencia en el mercado.

e. Estándares
   Toda adquisición se basa en los estándares, definida por la División de Informática.

f. Capacidades
   Se deberá analizar si satisface la demanda actual con un margen de holgura y capacidad de crecimiento para soportar la carga de trabajo del área. Para la adquisición de hardware se tendrá en cuenta lo siguiente:
   - El equipo que se desee adquirir deberá estar dentro de las listas de ventas vigentes de los fabricantes y/o distribuidores del mismo y dentro de los estándares del MAG.
   - Los equipos complementarios deberán tener una garantía mínima de un año y deberán contar con el servicio técnico correspondiente en el país.
   - La marca de los equipos o componentes deberá contar con presencia y permanencia demostrada en el mercado nacional, así como con asistencia técnica y de repuestos local. Tratándose de microcomputadores, a fin de mantener actualizada la arquitectura informática del MAG, la División de Informática emitirá anualmente las especificaciones técnicas mínimas para su adquisición.
   - Los dispositivos de almacenamiento, así como las interfaces de entrada/salida, deberán estar acordes con la tecnología de punta vigente, tanto en velocidad de transferencia de datos, como en procesamiento.
   - Las impresoras deberán apegarse a los estándares de Hardware y Software vigentes del mercado y a los del MAG, verificando que los suministros (cintas, papel, etc.) se consigan fácilmente en el mercado y no estén sujetas a un solo proveedor.
   - Conjuntamente con los equipos, se deberá adquirir el equipo complementario adecuado para su correcto funcionamiento de acuerdo con las especificaciones de los fabricantes, y que esta adquisición se manifieste en el costo de la partida inicial.
   - Los equipos adquiridos deben contar con asistencia técnica durante la instalación de los mismos.
   - En lo que se refiere a los servidores, equipos de comunicaciones, concentradores, switches y otros equipos que se justifiquen por ser de operación crítica y/o de alto costo, deben de contar con un programa de mantenimiento preventivo y correctivo que incluya el suministro de repuestos al vencer su período de garantía.
   - Al vencer la garantía de las computadoras personales por adquisición, deberán de contar por lo menos con un programa de servicio de mantenimiento correctivo que incluya el suministro de repuestos.

- Todo proyecto de adquisición de bienes de tecnología, debe sujetarse al análisis y visto bueno de la División de Informática.

g. Software

i. En la adquisición de equipo informático se deberá incluir el software vigente instalado con su licencia correspondiente.

ii. Los productos software autorizados para la adquisición se incluirán en el instructivo de estándares. Los tipos de productos son: sistemas operativos, bases de datos, lenguajes y herramientas de programación, utilitarios de oficina, Programas antivirus, correo electrónico, navegadores de internet y software para el diseño gráfico.

Licenciamiento.

4.9 Todos los productos de software que se utilicen contarán con su factura y licencia de uso respectiva; por lo que se promoverá la regularización o eliminación de los productos que no cuenten con el debido licenciamiento.

4.10 El Área de Infraestructura informática promoverá y propiciará que la adquisición de software de dominio público provenga de sitios oficiales y seguros.

Bases de datos

4.11 Para la operación del software de red en caso de manejar los datos mediante sistemas de información, se deberá tener en consideración lo siguiente:

i. Toda la información de la institución deberá invariablemente ser operada a través de un mismo tipo de sistema manejador de base de datos para beneficiarse de los mecanismos de integridad, seguridad y recuperación de información en caso de presentarse alguna falla.

ii. El acceso a los sistemas de información, deberá contar con los privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad total de la información de la institución. Los niveles de seguridad de acceso deberán controlarse por un administrador único y manipulado por software.

iii. Se deben delimitar las responsabilidades en cuanto a quién está autorizado a consultar y/o modificar en cada caso la información, tomando las medidas de seguridad pertinentes.

iv. Los datos de los sistemas de información, deben ser respaldados de acuerdo a la frecuencia de actualización de sus datos, guardando respaldos históricos periódicamente. Es indispensable llevar una bitácora oficial de los respaldos realizados, asimismo, los CD´s, DVDs Blue Ray de respaldo deberán guardarse en un lugar de acceso restringido con condiciones ambientales suficientes para garantizar su conservación. En cuanto a la información de los equipos de cómputo personales, se recomienda a los usuarios que realicen sus propios respaldos en los servidores de respaldo externo o en medios de almacenamiento alternos.

v. Todos los sistemas de información que se tengan en operación, deberán contar con sus respectivos manuales actualizados. Un técnico que describa la estructura interna del sistema así como los programas, catálogos y archivos que lo conforman y otro que describa a los usuarios del sistema asi como los procedimientos para su utilización.

vi. Los sistemas de información, deben contemplar el registro histórico de las transacciones sobre datos relevantes, así como la clave del usuario y fecha en que se realizó.

vii. Se deben implantar rutinas periódicas de auditoría a la integridad de los datos y de los programas de cómputo, para garantizar su confiabilidad.

V. POLITICAS DE SEGURIDAD

Políticas de seguridad física

Acceso Físico

5.1 El MAG destinará un área que servirá como centro de telecomunicaciones donde ubicarán los sistemas de telecomunicaciones y servidores.

5.2 Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada de manera que el usuario no tenga acceso físico directo. Entendiendo por sistema de comunicaciones: el equipo activo y los medios de comunicación.

5.3 El acceso de terceras personas debe ser identificado, controlado y vigilado durante el acceso portando una identificación que les será asignado por el área de seguridad de acceso al edificio y por las oficinas de la institución.

5.4 Las visitas internas o externas podrán acceder a las áreas restringidas siempre y cuando se encuentren acompañadas cuando menos por un responsable del área de infraestructura informática.

5.5 Para realizar el traslado o cambio de computadoras personales en las oficinas descentralizadas se necesita la autorización del jefe de la unidad o el Director de la oficina o dependencia, para el equipo informático, tipo servidores y de comunicación, se realizará con la autorización del Jefe de la División de Informática o Director la OGA. Se utilizarán los procedimientos y formatos de entrada/salida del Área de Activo Fijo.

Protección Física.

Data Center

5.6 El Data Center deberá:

a. Tener una puerta de acceso para favorecer el control del uso de los recursos informáticos.
b. Ser un área restringida. Tener un sistema de control de acceso que garantice la entrada solo al personal autorizado por el Jefe de la División.
c. Recibir limpieza al menos una vez por semana, que permita mantenerse libre de polvo.
d. Estar libre de contactos e instalaciones eléctricas en mal estado.
e. Poseer aire acondicionado.
f. Asignar un técnico para que realice un control diario temperatura y aires acondicionados y llevar un registro de estos controles.
g. Poseer un respaldo de energía redundante.
h. Seguir los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores.
i. Los sistemas de tierra física, sistemas de protección e instalaciones eléctricas deberán recibir mantenimiento anual con el fin de determinar la efectividad del sistema.
j. Contar con algún esquema que asegure la continuidad del servicio.
k. Prevenir o detector de incendios.
l. Contar con sistemas de extinción.
m. Contar por lo menos con dos extintores de incendio adecuado y cercano al Data Center.

Infraestructura tecnológica

5.7 Las dependencias deberán considerar los estándares vigentes de cableado estructurado durante el diseño de nuevas áreas o en el crecimiento de las áreas existentes.

Instalaciones de equipos informáticos

5.8 La instalación del equipo informático quedará sujeta a los siguientes lineamientos:

a. El Área de Infraestructura Informática deberán contar con un plano actualizado de las instalaciones eléctricas y de comunicaciones del equipo de cómputo en red.
b. Las instalaciones eléctricas y de comunicaciones, estarán preferiblemente fijas o en su defecto resguardadas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.
c. Las instalaciones se apegarán estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios.
d. En ningún caso se permitirán instalaciones improvisadas o sobrecargadas.
e. La supervisión y control de las instalaciones se llevará a cabo en los plazos y mediante los mecanismos que establezca el Jefe de la División de Informática.

Control

5.9La División de Informática y el Área de Activo Fijo llevará un control de los recursos informáticos y licenciamiento.

5.10 El encargado del Soporte Técnico es el responsable de organizar al personal del mantenimiento preventivo y correctivo de los equipos de cómputo.

5.11 La División de Recursos Humanos reportará a la División de Informática cuando un usuario deje de laborar en la institución a fin de retirarle las credenciales de ingreso a los recursos y supervisar la correcta devolución de los equipos y recursos asignados al usuario.

Respaldos.

5.12 Las Bases de Datos del MAG serán respaldadas periódicamente en forma automática y manual, según los procedimientos generados para tal efecto.

5.13 La División de Informática procurará contar con servidores de contingencia, lo que dependerá de la disponibilidad de los recursos financieros de la institución.

5.14 Para reforzar la seguridad de la información, los usuarios, bajo su criterio, deberán hacer respaldos de la información en sus discos duros frecuentemente, dependiendo de la importancia y frecuencia de cambio. Los respaldos serán responsabilidad absoluta de los usuarios.

5.15 El administrador del correo electrónico podrá remover información de cuentas individuales, cuando ésta sea ilegal, o ponga en peligro el buen funcionamiento de los sistemas, o se sospeche de algún intruso utilizando una cuenta ajena.

Recursos de los usuarios.

Uso

5.16 Los usuarios deberán cuidar, respetar y hacer un uso adecuado de los recursos informáticos de la institución, de acuerdo a las políticas de este documento.

5.17 Los usuarios deberá solicitar apoyo a la División de Informática ante cualquier duda en el manejo de los recursos informáticos de la institución.

5.18 El correo electrónico no se deberá usar para envío masivo, materiales de uso no institucionales o innecesarios (entiéndase cadenas, publicidad y propaganda comercial, política, social entre otras).

5.19 Los usuarios utilizarán los programas informáticos sólo en virtud de los acuerdo de licencia y no instalarán copias de los mismos.

5.20 Queda prohibido inspeccionar, copiar y almacenar programas de cómputo, software y demás fuentes que violen la ley de derechos de autor.

5.21 Los usuarios no podrán descargar de internet programas informáticos que no tengan autorización de la División de Informática, como los que utilizan sistemas de peer-to-peer (ejemplo Kazaa) que pueden utilizarse para comercializar trabajos protegidos por los derechos de autor, archivos de música (MP3, WAV, etc) de los cuales no es el autor o bien no posee los derechos de distribución del mismo.

5.22 Los técnicos de la División de Informática realizarán muestreos aleatorios para verificar la legalidad de la instalación del software.

Políticas de seguridad lógica

Red

5.23 Las redes tienen como propósito principal servir en la transformación e intercambio de información dentro y fuera del ministerio.

5.24 La División de Informática no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.

5.25 Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del responsable del equipo.

5.26 No se permite el uso de los servicios de la red cuando no cumplan con las labores propias del MAG.

5.27 Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos del usuario.

5.28 El uso de analizadores de red es permitido única y exclusivamente por el personal de la División de Informática para monitorear la funcionalidad de las redes, contribuyendo a la consolidación del sistema de seguridad.

5.29 Cuando se detecte un uso no aceptable, se cancelará la cuenta o se desconectará temporal o permanentemente al usuario o red involucrada dependiendo de las políticas. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.

Servidores

Configuración e instalación

5.30 Los técnicos del Área de Infraestructura Informática tienen la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la Red.

5.31 La instalación y/o configuración de todo servidor conectado a la Red será responsabilidad de los técnicos del Área de Infraestructura Informática.

5.32 Durante la configuración de los servidores, los técnicos informáticos deben generar las normas para el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los usuarios.

5.33 Los servidores que proporcionen servicios a través de la red e Internet deberán:

a. Funcionar 24 horas del día los 365 días al año
b. Recibir mantenimiento preventivo mínimo dos veces al año.
c. Recibir mantenimiento anual que incluya depuración de logs y la revisión de su configuración.

5.34 La información de los servidores deberá ser respaldada de acuerdo con los siguientes criterios, como mínimo:
a. Diariamente, información crítica
b. Semanalmente, los documentos web
c. Mensualmente, configuración del servidor y logs

5.35 El servicio de internet sólo podrá proveerse a través de los servidores autorizados por la División de Informática.

Correo electrónico

5.36 El Área de Infraestructura informática se encargará de la administración de las cuentas de correo electrónico en los servidores que administra.

5.37 Para efecto de asignarle su cuenta de correo al usuario, la División de Recursos Humanos, el Director de la oficina o dependencia que reciba al nuevo empleado solicitará a la División de Informática, dicha asignación.

5.38 El usuario cambiará la contraseña asignada inicialmente, al momento de ingresar a su cuenta de correo.

5.39 La longitud mínima de las contraseñas será igual o superior a ocho caracteres.

Bases de Datos

5.40 El administrador de la base de datos no deberá eliminar ninguna información del sistema, a menos que la información esté dañada o ponga en peligro el buen funcionamiento del sistema.

5.41 El administrador de la base de datos es el encargado de asignar las cuentas a los usuarios para el uso.

5.42 Las contraseñas serán asignadas por el Administrador de la Base de Datos en el momento en que el usuario desee activar su cuenta, previa solicitud al responsable de acuerdo al procedimiento generado.

5.43 En caso de olvido de contraseña de un usuario, será necesario que se presente con el Administrador de la Base de Datos para reasignarle su contraseña.

5.44 La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.

Recursos Informáticos

Seguridad

5.45 La División de Informática son los encargados de suministrar medidas de seguridad adecuadas contra la intrusión o daños a la información almacenada en los sistemas así como la instalación de cualquier herramienta, dispositivo o software que refuerce la seguridad de la información. Sin embargo, debido a la cantidad de usuarios y a la amplitud y constante innovación de los mecanismos de ataque no es posible garantizar una seguridad completa.

5.46 La División de Informática debe mantener informados a los usuarios y poner a disposición de los mismos el software que refuerce la seguridad de los sistemas de información.

5.47 La División de Informática es la única autorizada para monitorear constantemente el tráfico de paquetes sobre la red, con el fin de detectar y solucionar anomalías, registrar usos indebidos o cualquier falla que provoque problemas en los servicios de la red.

Técnicos de soporte

5.48 Los técnicos de soporte informático tendrán las siguientes responsabilidades:

a. Podrán ingresar de forma remota a computadoras únicas y exclusivamente para la solución de problemas y bajo solicitud explícita del propietario de la computadora.
b. Deberán utilizar los analizadores previa autorización del usuario y bajo la supervisión de éste, informando de los propósitos y los resultados obtenidos.
c. Realizar la instalación o adaptación de sus sistemas de información de acuerdo con los requerimientos en materia de seguridad.
d. Reportar a la Jefatura de la División de Informática sobre los incidentes de violación de seguridad de los recursos informáticos.

Renovación de equipos

5.49 Cuando las áreas requieran de un equipo para el desempeño de sus funciones ya sea por sustitución o para el mejor desempeño de sus actividades éstas deberán realizar una consulta al área de Soporte Técnico o consultar el Instructivo de Estándares Informáticos, a fin de que se seleccione el equipo adecuado.

Uso de los Servicios de Red

5.50 La División de Informática conjuntamente con la Dirección de la Oficina General de Administración definirán los servicios de Internet de acuerdo a las necesidades institucionales y a la disponibilidad financiera de la institución; asimismo coordinará con las demás jefaturas su otorgamiento y configuración.

5.51 Si usuarios externos y/o visitas desean utilizar los servicios de internet, deberán solicitarlo a la División de Informática.

5.52 No se proporcionarán equipo, contraseñas ni cuentas de correo a personas que presten servicio social o estén haciendo prácticas profesionales, excepto cuando sea solicitado del Director dónde prestan su servicio y autorizado por la Jefatura de Informática.

5.53 El administrador de servidor realizará las siguientes tareas:

a. Respaldo de información conforme a los procedimientos establecidos.
b. Revisión de logs y reporte de cualquier eventualidad.
c. Implementar de forma inmediata las recomendaciones de seguridad y reportar posibles faltas a las políticas de seguridad informáticas.
d. Monitoreo de los servicios de red proporcionados por los servidores a su cargo.
e. Organizar y supervisar al personal encargado del mantenimiento preventivo y correctivo de los servidores.

5.54 Podrán aislar cualquier servidor de red, notificando al Director de la OGA y a los usuarios, en las condiciones siguientes:

a. Si los servicios proporcionados por el servidor implican un tráfico adicional que impida un buen desempeño de la Red.

b. Si se detecta la utilización de vulnerabilidades que puedan comprometer la seguridad en la Red.
c. Si se detecta la utilización de vulnerabilidades que puedan comprometer la seguridad de la Red.
d. Si se detecta la utilización de programas que alteren la legalidad y/o consistencia de los servidores.
e. Si se detectan accesos no autorizados que comprometan la integridad de la información.
f. Si se viola las políticas de uso de los servidores.
g. Si se reporta un tráfico adicional que comprometa a la red de la institución.

5.55 El Administrador de Servidor es el único autorizado para asignar las cuentas a los usuarios.

Usuarios

Identificación de usuarios y contraseñas

5.56 Todos los usuarios con acceso a un sistema de información o a la Red, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.

5.57 El usuario deberá definir su contraseña de acuerdo al procedimiento establecido para tal efecto y será responsable de la confidencialidad de la misma.

5.58 Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por la División de Informática.

5.59 La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos y numéricos.

5.60 Los identificadores para usuarios temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.

5.61 El usuario deberá renovar su contraseña y colaborar en lo que sea necesario, a solicitud de la División de Informática, con el fin de contribuir a la seguridad de los servidores en los siguientes casos:
a. Cuando ésta sea una contraseña débil o de fácil acceso.
b. Cuando crea que ha sido violada la contraseña de alguna manera.

5.62 El usuario deberá notificar al Área de Infraestructura Informática en los siguientes casos:
a. Si observa cualquier comportamiento anormal (mensajes extraños, lentitud en el servicio o alguna situación inusual) en el servidor.
b. Si tiene problemas en el acceso a los servicios proporcionados por el servidor.

Responsabilidades Personales

5.63 Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.

5.64 Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.

5.65 Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.

5.66 Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña e informar a su jefe inmediato y éste reportar al responsable de la administración de la red.

5.67 El usuario debe utilizar una contraseña compuesta por un mínimo de ocho caracteres constituida por una combinación de caracteres alfabéticos y numéricos.

5.68 La contraseña no debe hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fecha significativas, días de la semana, meses del año, nombre de personas, teléfonos.

5.69 En caso que el sistema no lo solicite automáticamente, el usuario debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.

5.70 En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada seis meses.

5.71 Proteger, en la medida de sus posibilidades, los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentren contenidos los datos.

Uso apropiado de los Recursos.

5.72 Los Recursos Informáticos, Datos, Software, Red y Sistemas de Comunicación están disponibles exclusivamente para complementar las obligaciones y propósito de la operativa para la que fueron diseñados e implantados. Todo el personal usuario de dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso.

5.73 Prohibiciones

a. El uso de estos recursos para actividades no relacionadas con la misión de la institución.
b. Las actividades, equipos o aplicaciones que no estén directamente especificados como parte del Software o de los Estándares de los Recursos Informáticos propios del Ministerio.
c. Introducir en los Sistemas de Información o la Red Corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.
d. Introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los Recursos Informáticos.
e. Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.
f. Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.
g. Albergar datos de carácter personal en las unidades locales de disco de los computadores de trabajo.
h. Cualquier fichero introducido en la Red o en el puesto de trabajo del usuario a través de soportes automatizados, internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas Políticas y, en especial, las referidas a propiedad intelectual y control de virus.

Responsabilidad de los técnicos informáticos del MAG

5.74 Los técnicos informáticos serán responsables de:

a. Implementar la Solución Antivirus en las computadoras del MAG.
b. Solucionar contingencias presentadas ante el surgimiento de virus que la solución no se haya detectado automáticamente.
c. Configurar el analizador de red para la detección de virus.

5.75 Los técnicos de soporte aislarán el equipo notificando al Jefe de Informática, en las condiciones siguientes:
a. Cuando la contingencia con virus no es controlada, con el fin de evitar la propagación de virus a otros equipos y redes.
b. Si el usuario viola las políticas antivirus.
c. Cada vez que los usuarios requieran hacer uso de discos, USB's, éstos serán rastreados por la Solución Antivirus en la computadora del usuario o en un equipo designado para tal efecto en las áreas de cómputo de las dependencias.

5.76 En caso de contingencia con virus los técnicos de soporte deberán seguir el procedimiento establecido.

Políticas sobre el Antivirus

5.77 Antivirus de la Red
a. Todos los equipos de cómputo del MAG deberán tener instalada una Solución de Antivirus.
b. Periódicamente se hará el rastreo en los equipos de cómputo del MAG, se realizará la actualización de las firmas de antivirus proporcionadas por el fabricante de la solución antivirus en los equipos conectados a la Red.

5.78 Todos los equipos de cómputo conectados al dominio deben tener instalado y actualizado el programa de antivirus, con el fin de que esto sea cumplido, cualquier proceso interno de asignación y/o rotación de equipos de cómputo. La desinstalación del antivirus se encuentra restringida a la validación de clave de desinstalación, la cual se encuentra a disposición únicamente del equipo de soporte interno.

5.79 El usuario no deberá desinstalar la solución antivirus de su computadora pues ocasiona un riesgo de seguridad ante el peligro de virus.

5.80 Si el usuario hace uso de medios de almacenamiento personales, éstos serán rastreados por la Solución de Antivirus en la computadora del usuario o por el equipo designado para tal efecto.

5.81 El usuario deberá comunicarse con los técnicos de soporte en caso de problemas de virus para buscar la solución.

5.82 El usuario será notificado por los técnicos de soporte en los siguientes casos:
a. Cuando sea desconectado de la red con el fin de evitar la propagación del virus a otros usuarios de la red.
b. Cuando sus archivos resulten con daños irreparables por causa de virus
c. Cuando viole las políticas antivirus.

Seguridad Perimetral

5.83 La seguridad perimetral es uno de los métodos posibles de protección de la Red, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles. Esto permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

5.84 Los técnicos del Área de Infraestructura informática implementarán soluciones lógicas y físicas que garanticen la protección de la información del MAG contra posibles ataques internos o externos, como las siguientes:

a. Rechazar conexiones a servicios comprometidos
b. Permitir sólo ciertos tipos de tráfico, como el correo electrónico, http y https.
c. Proporcionar un único punto de interconexión con el exterior.
d. Redirigir el tráfico entrante a los sistemas adecuados dentro de la Red Interna.
e. Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet.
f. Auditar el tráfico entre el exterior y el interior.
g. Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red cuentas de usuarios internos.

Firewall

5.85 La solución de seguridad perimetral debe ser controlada con un Firewall por hardware (físico) que se encarga de controlar puertos y conexiones, es decir, de permitir el paso y el flujo de datos entre los puertos, ya sean clientes o servidores.

5.86 Los técnicos de Infraestructura informática establecerán las reglas en el Firewall necesarias para bloquear, permitir o ignorar el flujo de datos entrante y saliente de la Red.

5.87 El firewall debe bloquear las conexiones extrañas y no dejarlas pasar para que no causen problemas.

5.88 El firewall debe controlar los ataques de "Denegación de Servicio" y controlar también el número de conexiones que se están produciendo, y en cuanto detectan que se establecen más de las normales desde un mismo punto bloquearlas y mantener el servicio a salvo.

5.89 Controlar las aplicaciones que acceden a Internet para impedir que programas a los que no hemos permitido explícitamente acceso a Internet, puedan enviar información interna al exterior.

Sistemas de Detección de Intrusos (ID)

5.90 Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es una aplicación usada para detectar accesos no autorizados a un computador/servidor de una red. Estos accesos pueden ser ataques realizado por usuarios malintencionados con conocimientos de seguridad o a través de herramientas automáticas.

5.91 Los técnicos de Infraestructura informática implementarán soluciones lógicas y físicas que impidan el acceso no autorizado a los equipos del MAG:

a. Detección de ataques en el momento que están ocurriendo o poco después.
b. Automatización de la búsqueda de nuevos patrones de ataque, con herramientas estadísticas de búsqueda y al análisis de tráfico anómalo.

c. Monitorización y análisis de las actividades de los usuarios en busca de elementos anómalos.
d. Verificación de configuraciones y vulnerabilidades de los sistemas.
e. Descubrir sistemas con servicios habilitados que no deberían tener, mediante el análisis del tráfico y de los logs.
f. Análisis de comportamiento anormal. Si se detecta una conexión fuera de hora, reintentos de conexión fallidos y otros, existe la posibilidad de que se esté en presencia de una intrusión. Un análisis detallado del tráfico y los logs puede revelar una máquina comprometida o un usuario con su contraseña al descubierto.
g. Automatizar tareas como la actualización de reglas, la obtención y análisis de logs, la configuración de cortafuegos.
h. La Red del MAG sólo podrá acceder a los parámetros que el Firewall tenga permitido o posibilite mediante su configuración.

Conectividad a Internet

5.92 La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Todos los colaboradores de la institución tienen las mismas responsabilidades en cuanto al uso de Internet.

5.93 El acceso a Internet se restringe exclusivamente a través de la Red establecida para ello, es decir, por medio del sistema de seguridad con el Firewall incorporado en la misma.

5.94 No está permitido acceder a Internet llamando directamente a un proveedor de servicio de acceso y usando un navegador, o con otras herramientas de Internet conectándose con un módem.

5.95 Internet es una herramienta de trabajo. Todas las actividades en Internet deben estar en relación con tareas y actividades del trabajo desempeñado.

5.96 Sólo puede haber transferencia de datos de o a Internet en conexión con actividades propias del trabajo desempeñado.

Red Inalámbrica (WIFI)

Acceso a funcionarios

5.97 La red inalámbrica es un servicio que permite conectarse a la red del MAG e Internet sin la necesidad de algún tipo de cableado. La Red inalámbrica le permitirá utilizar los servicios de Red, en las zonas de cobertura de la institución.

5.98 Donde además de hacer uso del servicio de acceso a los sistemas, podrán acceder al servicio de Internet de manera controlada.

5.99 Las condiciones de uso presentadas definen los aspectos más importantes que deben tenerse en cuenta para la utilización del servicio de red inalámbrica, estas condiciones abarcan todos los dispositivos de comunicación inalámbrica (computadoras portátiles, Ipod, celulares, etc.) con capacidad de conexión Wireless.

a. El Administrador del servidor de red es el encargado de la administración, habilitación y/o bajas de usuarios en la red inalámbrica del MAG.

Seguridad

5.100 El administrador del Servidor de dominio determinará las medidas pertinentes de seguridad para usar las redes inalámbricas.

5.101 El administrador del Servidor de dominio se reserva el derecho de llevar un registro de los eventos asociados a la conexión de los diferentes usuarios para asegurar el uso apropiado de los recursos de red. No se deben realizar intentos de ingreso no autorizado a cualquier dispositivo o sistema de la red inalámbrica. Cualquier tipo de ingreso no autorizado es una práctica ilegal.

5.102 No se debe hacer uso de programas que recolectan paquetes de datos de la red inalámbrica.

5.103 Con la finalidad de evitar responsabilidades, en caso de que algún usuario haga cambio de cualquiera de los equipos previamente dado de alta, este necesariamente deberá comunicar a la División de Informática y al Área de Activo Fijo para su respectiva baja del equipo de la red inalámbrica.

Tecnología

5.104 La Red inalámbrica del MAG sólo soporta el protocolo TCP/IPV.4 en la red inalámbrica.

5.105 La División de Informática se reserva el derecho de limitar los anchos de banda de cada conexión según sea necesario, para asegurar la confiabilidad y desempeño de la red y de esta manera garantizar que la red sea compartida de una manera equitativa por todos los usuarios de la institución.

5.106 No se permiten la operación ni instalación de puntos de acceso conectados a la red cableada del MAG sin la debida autorización por parte del Jefe de Informática.

Restricciones y prohibiciones de acceso a Internet

5.107 Con la finalidad de hacer un buen uso de la red inalámbrica, se aplicarán las siguientes prohibiciones:

a. El uso de programas para compartir archivos (Peer to Peer).
b. El acceso a páginas con cualquier tipo de contenido explícito de pornografía.
c. El uso de sitios de videos en línea o en tiempo real.
d. Debido a las limitaciones de ancho de banda existentes NO se permite la conexión a estaciones de radio por Internet.
e. Uso de JUEGOS on line en la red.

Excepciones

5.108 Entre las medidas de seguridad se encuentran configurado para restringir algunas palabras y sitios de Internet; por lo que pueden existir palabras o sitios que a pesar de ser inofensivos tendrán negado el acceso; en este caso, los usuarios podrán notificar a través de nota, esta situación para que sea resuelta.

5.109 En caso de eventos, cursos, talleres, conferencias, etc. Se podrá habilitar equipos de manera temporal por el tiempo necesario previa solicitud del jefe de oficina interesada con una anticipación de por lo menos un día hábil.

Control Interno

5.110 El sistema de control interno de la División de Informática será evaluado al menos una vez por año y se modificará de acuerdo a los resultados.

Acceso a Invitados

5.111 La red inalámbrica es un servicio que permite conectarse al personal externo del ministerio a internet sin la necesidad de algún tipo de cableado. La Red inalámbrica de invitados le permitirá utilizar los servicios de Internet, en las zonas de cobertura de la institución.

5.112 Los usuarios invitados no tendrán acceso a la red ni a ningún recurso de uso privado del MAG.

VI. PLAN DE CONTINGENCIAS

El Plan de contingencias de la División de Informática estará incluido en el Plan de contingencias de la Oficina General de Administración.

VII. VIGENCIA Y ACTUALIZACION DE LA POLITICA DE SEGURIDAD

Debido a la propia evolución de la tecnología y las amenazas de seguridad, y a las nuevas aportaciones legales en la materia, está políticas se modificará cuando sea necesario. Los cambios realizados en esta Política serán divulgados a todos los usuarios del MAG.
Es responsabilidad de cada uno de los usuarios la lectura y conocimiento de la Política de Seguridad y sus modificaciones.

COMUNÍQUESE. Licenciado Orestes Fredesman Ortez Andrade, Ministro de Agricultura y Ganadería. (f) Fredesman Ortez".

El que transcribo a usted para su conocimiento y efectos consiguientes.

DIOS UNION LIBERTAD

Lic. Walter Menjívar
Director General de Administración y Finanzas