SERVICIO NACIONAL DE METEOROLOGIA E HIDROLOGIA - SENAMHI -

OFICINA GENERAL DE ESTADISTICA E INFORMATICA
RESOLUCION JEFATURAL No.0187 SENAMHI-JSS-OGEI/2005
LIMA 22 DE AGOSTO DE 2005

CONSIDERANDO:

Que, como parte de la modernización de la capacidad tecnológica para el desarrollo integral del SENAMHI, se vienen desarrollando sistemas informáticos aplicativos para la mejora continua de los procesos productivos de las diferentes dependencias, las mismas que permiten su uso entre diferentes usuarios internos y externos de la Institución, con el objeto de dar mayor dinamismo y utilización de los servicios hidrometeorológicos y conexos para beneficio y desarrollo económico y social del país;

Que, los sistemas informáticos desarrollados deben estar a disposición del público usuario debidamente registrado en la Institución, con el fin de que se cumpla con las medidas de seguridad y las aplicaciones a nivel de consulta que beneficien a la población y a los sectores económicos y productivos en el menor plazo posible, mediante los diferentes medios de comunicación a nivel de Internet, Intranet y Acceso Remoto, que viene implementando el SENAMHI;

Que, es necesario aprobar la Directiva que establezca las normas especificas y responsabilidades para la utilización de los medios de comunicación informática implementados en la Institución, la misma que ha sido propuesta por la Oficina General de Estadística e Informática;

Estando a lo acordado con la Oficina General de Estadística e Informática, Oficina de Racionalización, Oficina de Asesoría Jurídica, el visto bueno de la Dirección Técnica del Servicio y de acuerdo al Decreto Supremo Nº 074-95-PCM, que establece la responsabilidad exclusiva de cada Entidad del Sector Público de aprobar sus instrumentos de Gestión Institucional y a las facultades conferidas por la Resolución Suprema Nº 092-2005-DE/FAP-CP del 19 de enero de 2005;

SE RESUELVE:

ARTICULO 1º.- APROBAR la Directiva sobre "Normas Especificas para la Utilización del Internet, Intranet y Acceso Remoto a la Información Hidrometeorológica y Conexa del SENAMHI", la misma que forma parte integrante de la presente Resolución.

ARTICULO 2º.- DISPONER la publicación de la presente Directiva en el Portal WEB del SENAMHI.

Regístrese, comuníquese, publíquese y archívese.

El Mayor General FAP
JUAN OVIEDO MOTTA
Jefe del SENAMHI

Distribución:
Copia DTS - ORA
OGEI.
TODAS LAS DEPENDENCIAS DEL SENAMHI.
Archivo.
18.08.05
AR/WLM/MPH

Oficina General de Estadística e Informática
Reg. N° 748
Fecha 23/08/05

Lima, 22 DE AGOSTO DE 2005

DIRECTIVA Nº 017 JSS-DTS-OGEI/2005

NORMAS ESPECIFICAS PARA LA UTILIZACIÓN DEL INTERNET, INTRANET Y ACCESO REMOTO A LA INFORMACIÓN HIDROMETEOROLÓGICA Y CONEXA DEL SENAMHI

1. OBJETIVO

Establecer las normas especificas para la utilización del Internet, Intranet y el acceso remoto a la información hidrometeorológica y conexa del SENAMHI.

2. FINALIDAD

a. Usar adecuadamente los medios de información a través del Internet e Intranet en las dependencias autorizadas y validadas por el SENAMHI.

b. Estandarizar los procedimientos y limitaciones para el acceso remoto en línea a la información hidrometeorológica.

c. Disponer de un medio para el acceso remoto a la información procesada hidrometeorológica y conexas del SENAMHI, permitiendo su disponibilidad en tiempo real por las dependencias autorizadas y validadas.

d. Aprovechar la disponibilidad para compartir estos medios para la explotación de la información entre todas las dependencias del SENAMHI y otras dependencias autorizadas y validadas.

3. BASE LEGAL

a. Inciso b), g) y e) del Artículo 4º de la Ley 24031, Ley del SENAMHI.
b. Inciso a) del Artículo 2º, Artículo 8º de Ley Nº 28493, Ley que regula el Uso del Correo Electrónico Comercial no solicitado.
c. Resolución Jefatural Nº 234-2001-INEI, que aprueba la Directiva Nº 016-2001-INEI/DTNP, Normas y Procedimientos Técnicos sobre Contenidos de las Páginas WEB de las Entidades de la Administración Pública.

d. Resolución Ministerial Nº 662-96-MTC/15.17, que aprueba la Directiva Nº 002-96-MTC/15.17, sobre Procedimientos de Inspección y de Requerimiento de Información en Relación al Secreto de las Telecomunicaciones y la Protección de Datos.
e. Resolución Jefatural Nº 340-94-INEI, que aprueba la Directiva Nº 015-94-INEI/SJI, Normas Técnicas para el Almacenamiento y Respaldo de la Información que se Procesa en las Entidades del Estado.

4. ALCANCE

La presente Directiva es de cumplimiento de todas las dependencias del SENAMHI y otras dependencias que son autorizadas y validadas por la Alta Dirección.

5. VIGENCIA

La presente Directiva entra en vigencia a partir de la aprobación de la respectiva Resolución Jefatural.

6. NORMAS ESPECIFICAS

a. Información confidencial y legal del SENAMHI.

Toda Información relacionada a la operación y funcionamiento de la institución, es confidencial y constituye secreto de ésta, permanece como propiedad o negocio de la institución y está sujeta a derechos de propiedad intelectual, duplicidad o protección similar.

b. Seguridad tecnológica del Sistema Informático.

1) Cada elemento, producto y servicio de la Infraestructura Tecnológica de la institución, tiene un usuario identificado y registrado en la Oficina General de Estadística e Informática como responsable directo para el uso de los recursos informáticos, así como para dar cumplimiento a las políticas de protección y seguridad de los mismos.

2) Todos los equipos de comunicación, incluyendo el ruteador de conexión a Internet e Intranet, contarán con una clave de seguridad (password) que será del tipo alfanumérica y cambiada periódicamente.

3) La claves deberán ser definidas y administradas por el Área de Redes y no serán conocidas y/o usadas por más de tres (3) personas; serán además diferentes entre sí y se entregará una copia escrita de éstas, en sobre cerrado a la Oficina de Informática.

4) La Oficina General de Estadística e Informática establece medidas de seguridad para que cada persona o usuario registrado, acceda a los recursos tecnológicos del SENAMHI y cuente con:

a) **Una identificación como usuario**: para su acceso controlado y limitado en los niveles que corresponda, manteniendo la integridad y seguridad del sistema.

b) **Autenticación**: para verificar al usuario mediante controles que permitan identificarlo antes de permitirse su acceso.

c) **Registro de Auditoría**: para que toda transacción que efectúe el usuario en la red informática, esté sujeto a control de auditoría y se grabe los accesos efectuados para revisiones de rutina o identificar actividades ilegales o inapropiadas realizadas. Los registros serán lo suficientemente detallados para facilitar la reconstrucción de los eventos realizados y verificar o no, la sospechas restablecidas para el sistema.

d) **Equipos**: para proporcionar la tecnología informática, con áreas de memoria o almacenamiento de datos (cintas, lectoras ópticas, etc.) inicializados y totalmente operativos.

e) **Control de accesos**: para que todo equipo sensible de la red esté implementado con medidas de seguridad adicionales para el control de accesos, como contraseñas (para acceder a archivos), listas de control de acceso, encriptación de disco u otras técnicas establecidas.

c. Enlace de telecomunicaciones entre la red informática de la institución e instituciones externas.

1) Todo enlace de telecomunicaciones entre la red informática de la institución e instituciones externas, contarán con la aprobación y autorización del Jefe del SENAMHI y será administrada por la Oficina General de Estadística e Informática.

2) Las condiciones para el enlace y conexión a la red informática cumplirán las siguientes condiciones básicas:

a) Los sistemas informáticos no críticos que se conecten en la red interna de la Institución, estará documentado localmente con manuales para el usuario, incluyendo la aprobación de la administración de seguridad y una descripción técnica de la conexión; es especial, para los servidores o estaciones de trabajo, que no contienen o procesan información sensible y no están conectadas físicamente o lógicamente a otra red.

b) Toda conexión de los sistemas informáticos de la Institución hacia otras redes, deberá ser aprobada por la Dirección u Oficina encargada de su actualización y mantenimiento de los aplicativos del sistema y autorizada por el Jefe del SENAMHI. La Oficina General de Estadística e Informática como administrador de la red institucional, garantizará las medidas de seguridad adecuadas para que toda la documentación pertinente, como contratos de licencia y acuerdos de interconexión, estén aprobados y autorizados por ambas partes.

d. Conexión a Internet en el SENAMHI.

1) La conexión a Internet en el SENAMHI, estará apropiadamente diseñada por la Oficina General de Estadística e Informática, para soportar los requerimientos tanto de los usuarios del SENAMHI como de usuarios externos.

2) Las condiciones para el enlace y conexión al Internet cumplirán con las siguientes condiciones básicas:

   a) Todos los usuarios, oficinas y áreas que requieran el acceso y/o conexión a Internet para implementar aplicaciones informáticas relativas a sus funciones, usarán este medio como punto de acceso, previa autorización de la Oficina General de Estadística e Informática del SENAMHI.

   b) Las conexiones para este tipo de aplicaciones, deberán emplear un equipo ruteador totalmente independiente de otros enlaces, tanto interno como externo.

   c) El ancho de banda de este enlace estará diseñado para soportar tanto el tráfico de entrada, como el tráfico de salida sin congestionar el tráfico normal que requiere la Institución.

   d) La Oficina de Estadística e Informática empleará algún tipo de utilitario, a fin de administrar el ancho de banda, dando prioridad a los servicios a clientes.

   e) La conexión estará ubicada en la Sede Central del SENAMHI; y en las DDRR, se contará con el soporte y control de la Oficina General de Estadística e Informática.

3) La Implementación de servicios de transferencia de archivos, para usuarios externos vía Internet, deberá ser realizada en una red independiente de la red LAN del SENAMHI y de ser necesario, se instalará un servidor FTP, en un segmento de red aislado y controlado por un firewall, a la que se le denominará "red perimetral o red desmilitarizada".

4) Los accesos de terminal remoto (TELNET), se bloquearán para los usuarios externos vía Internet del SENAMHI, mediante el firewall respectivo, permitiéndose sólo el empleo de este servicio, entre las diferentes áreas que conforman la red LAN/WAN del SENAMHI, a la que se denominará la "INTRANET del SENAMHI".

5) No se implementará ningún servicio accesible por Internet que dé información de los usuarios internos, como los servicios *finger, que* deben ser bloqueados y deshabilitados de los servidores UNIX, LINUX, Windows Server o cualquier otro sistema operativo que pueda brindar este servicio.

6) No está permitido el uso de servicios de conferencias en tiempo real por Internet, salvo al personal autorizado por la Alta Dirección del SENAMHI, y la distribución de cualquier información a través de este medio, estará sujeta a examen minucioso y aprobación del personal de administración de la red.

7) La información enviada, publicada y/o recibida vía Internet por el personal del SENAMHI, estará sujeta a un monitoreo y auditoría por parte del personal encargado de administración de la red, reservándose el SENAMHI, el derecho de determinar la conveniencia o no de la misma, así como de la confidencialidad de la información.

8) Se prohíbe el acceso a "sites" con contenido pornográfico y/o obsceno o servicios Internet, que proporcionen material pornográfico u otro material potencialmente ilegal o indeseable. El Administrador de la red aplicará los filtros necesarios para el bloqueo de estos "sites", e informará sobre las violaciones que efectúen los usuarios, para las medidas correctivas pertinentes.

9) El personal autorizado para el uso de Internet, podrá hacer uso "apropiado" dentro o fuera del horario de trabajo, los fines de semana y feriados para:

   a) Participar en asociaciones cívicas o profesionales.
   b) Conducta educativa o búsqueda de proyectos.
   c) Recuperación de novedades e información de interés general.

e. Difusión Web del SENAMHI.

1) La implementación de servicios WEB para usuarios externos vía Internet del SENAMHI, deberá ser realizada en una red independiente de la red LAN/WAN del SENAMHI, para lo cual el Servidor Web se debe instalar en un segmento de red aislado y controlado por un Firewall, a la que se denominará red "perimetral o red desmilitarizada".

2) La difusión Web del SENAMHI se hará usando su nombre DNS: www.senamhi.gob.pe En ningún caso se utilizará la numeración IP la misma que es de carácter reservado y de uso interno.

3) Para evitar violaciones a la seguridad del servidor Web, no se habilitará el servicio FTP.

f. Enlace dedicado a Internet como a enlaces externos y/o redes públicas.

1) En todo enlace dedicado, tanto a Internet como los enlaces externos y/o redes públicas, que empleen ruteadores, la Oficina General de Estadística e Informática deberá controlarlas empleando la tecnología de Firewall (corta fuego), para el respectivo control de acceso y/o tráfico.

2) Las condiciones para el enlace dedicado a Internet como a enlaces externos y/o redes públicas, cumplirán con las siguientes condiciones básicas:

   a) En la conexión con Internet se tendrá en cuenta el concepto de Firewall, para que el administrador de la red de la Oficina General de Estadística e Informática, tenga un control de acceso de los usuarios externos desde Internet, así como de los usuarios internos del SENAMHI.

   b) El firewall que se instale, deberá bloquear todo lo que no esté explícitamente permitido y esconder la estructura de la red del SENAMHI.

   c) La Oficina de Estadística e Informática estará encargada del mantenimiento de la Documentación y Sistemas del SENAMHI, así como de la administración de la seguridad de la red informática, incluyendo la

documentación de procedimientos de administración del firewall para la respuesta a un incidente de seguridad y la supervisión del mismo.

g. Restricciones para el uso de transferencia de archivos desde o hacia Internet.

1) No está permitido el uso de transferencia de archivos desde o hacia Internet a ninguna Dirección, Oficina, área o personal del SENAMHI, salvo que esté debidamente autorizado por la Alta Dirección.

2) La Alta Dirección No autorizará el uso de transferencia de archivos, previo informe de la Oficina de Estadística e Informática, cuando:

a) La transferencia de archivo de Internet (protocolo FTP) permita la posibilidad de transferir programas y/o archivos de diversas fuentes y lugares, cuyo uso está restringido sólo personal autorizado.

b) Los riesgos de carga e instalación de programas y archivos no autorizados en equipos de propiedad del SENAMHI, no impidan ingresos de virus al sistema informático o permitan riesgos por mal uso de los recursos de espacio en disco, tiempo de proceso y disponibilidad de ancho de banda tanto del enlace a Internet, como de los enlaces que conforman la red LAN del SENAMHI.

h. Rutas de acceso a un servicio determinado.

Las rutas de acceso a un servicio determinado, deberán minimizarse y sólo debe permitirse la entrada a un servicio critico de la red del SENAMHI, a través de un punto de acceso autorizado y controlado por medio de tecnologías de control de acceso (provistas por los firewalls) y monitores de intrusos.

i. Acceso remoto a la red LAN o por la Intranet del SENAMHI.

Todo acceso remoto a la red LAN del SENAMHI o la Intranet del SENAMHI tanto de los trabajadores del SENAMHI, como de personal externo autorizado, deberá ser fuertemente autenticado, mediante el empleo de passwords dinámicos de la tecnología de "tokens" o de fichas.

j. Sesión remota vía Tarantella, Messir Net y otros.

1) Toda sesión remota vía Tarantella, Messir Net u otros aplicativos que tengan funciones equivalentes, a través de una red pública a la red del SENAMHI mediante los protocolos de Internet, deberá trabajar en forma encriptada, empleando para ello tecnología de Redes Privadas Virtuales (VPNs) o aquellas que posibiliten un control centralizado de las mismas, para lo cual, la Oficina de Estadística e Informática deberá, incluir como parte de la respectiva transacción virtual, las instrucciones o normas para su utilización por parte de los usuarios.

2) La información que se otorgue por estos medios, será exclusivamente para el uso de los productos o resultados que se generan de las aplicaciones informáticas del SENAMHI y **no incluirá información básica o data hidrometeorológica y conexas**; para lo cual, la Oficina

General de Estadística e Informática incluirá los manuales y procedimientos para un mejor uso y entendimiento en la obtención de la información procesada que se requiera.

3) En estas sesiones de acceso remoto por medio del tarantella, Messir Net o Aplicativos equivalentes, se integrarán progresivamente los siguientes sistemas:

Sistema Estadístico
Sistema Climatológico
Sistema Fenológico
Sistema de Presupuesto
Sistema Consulta de Estaciones
Sistema Información Geográfica
Sistema de Control de Calidad de Datos (modo Consulta)
Otros sistemas que se implementen

k. Acceso a los servicios informáticos centrales del SENAMHI.

Todo acceso de terceros o clientes a los servicios informáticos centrales del SENAMHI, no debe ser directo y debe dirigirse a través de una entrada de aplicación (entrada de seguridad de comunicación, firewall o sistema intermedio) que refuerce las reglas de protección y seguridad establecidas.

l. Acceso al Correo Electrónico.

1) El correo electrónico será asignado a todos aquellos usuarios del SENAMHI que por funciones propias de su trabajo, tengan necesidad de esta comunicación. Para ello, cada Dirección u Oficina de la Institución, deberá formular la solicitud correspondiente a la Oficina General de Estadística e Informática, utilizando el formato "Solicitud de Servicios de Red", la misma que evaluada y aprobada, se autorizará su asignación.

2) La asignación del correo electrónico, implica que los trabajadores mientras permanezcan laborando en el SENAMHI, tendrán una dirección personal que les permita tanto el envío, como el recibo de correo electrónico de Internet (protocolo SMTP) y tendrán únicamente una cuenta de correo electrónico.

3) Las restricciones que se establezcan con respecto al uso de correo electrónico, serán comunicadas a los usuarios y estarán basadas en las consideraciones funcionales del personal, así como en la disponibilidad de recursos de espacio en disco del servidor de Correo Electrónico (servidor SMTP) y del ancho de banda de la conexión a Internet.

4) Todas las cuentas asignadas y correspondientes a una dirección tendrán una contraseña, la misma que puede ser cambiada cuantas veces lo considere conveniente el usuario. A los usuarios que no definan una contraseña, no se les garantizará la inviolabilidad de su información.

5) Todo mensaje de Correo Electrónico externo o interno de Internet deberá ser verificado por el administrador informático de la Oficina General de Estadística e Informática, con mecanismos de antivirus, para evitar que acceden a los sistemas internos.

6) La Oficina de Estadística e Informática establecerá y dispondrá de una política de antivirus, tanto para todas las estaciones de trabajo, como para los servidores, implementando de ser necesario, mecanismos complementarios a los Firewalls para bloquear y verificar los mensajes de correo electrónico de Internet (SMTP) contra los riesgos de virus informáticos y para lo cual la solución tendrá integración con la solución de firewall a implementar.

7) Todo mensaje de Correo Electrónico externo o interno de Internet, de confidencialidad o integridad alta, podrá ser enviado en forma encriptada, siendo potestad y responsabilidad del usuario, funcionario o Director que la envíe, estableciendo esta atribución.

8) Las Direcciones, oficinas o los funcionarios y personal autorizado del SENAMHI, que requiera enviar información de confidencialidad alta/media o de integridad alta/media por medio del correo electrónico a Internet, lo efectuarán en forma encriptada tanto el mensaje, el archivo adjunto al mensaje, o ambos, recomendándose la utilización de contraseña en los editores de texto, hojas de cálculo, etc. al guardar el documento a enviar.

m. Auditoria Interna de Seguridad

Periódicamente se realizarán Auditorias Internas de Seguridad de Internet e Intranet, Acceso Remoto (Tarantella, Messir NET), Correo Electrónico y la Web; para lo cual, se usará como herramienta de software, el Proxy Server entre otras, para descubrir las vulnerabilidades de seguridad existentes en los elementos de la Intranet del SENAMHI, en los Firewalls y en los Servidores Web.

7. NORMAS COMPLEMENTARIAS

a. De comprobarse alguna irregularidad en uso, aplicación, autorización del Internet, Intranet, Acceso Remoto o Información Hidrometeorológica o Ambiental por estos medios, por parte del personal del SENAMHI, así como por otro personal no autorizado, violando la seguridad de los mismos, para orientar o favorecer a terceros, así como para usufructuar estos medios para otras labores, trabajos o servicios no autorizados por el SENAMHI y que compitan con la Entidad, se aplicará la máxima sanción que establece el Reglamento Interno de Trabajo o las normas legales establecidas, sin perjuicio de que el SENAMHI formule la denuncia civil o penal que corresponda.

b. Las situaciones que no están explícitamente definidos o previstos en la presente Directiva, será resuelta por la Alta Dirección.

8. RESPONSABILIDADES

a. DE LA OFICINA GENERAL DE ESTADISTICA E INFORMATICA

1) Matricular a los nuevos usuarios y efectuar la baja correspondiente de la base de datos de contraseñas, previa evaluación y aprobación por la Alta Dirección.

2) Llevar el control de acceso diario, verificando el nivel de acceso.

3) Identificar las amenazas de seguridad y establecer medidas de protección para todos los recursos.

4) Cumplir y hacer cumplir las disposiciones normativas establecidas en la presente Directiva, asegurando que sean distribuidas y de conocimiento de todo el personal del SENAMHI y otros expresamente autorizados.

5) Administrar los Reportes de Seguridad.

6) Informar a la Alta Dirección cualquier incidente de seguridad, como intentos no-autorizados de acceso a información, infección de virus u otros eventos relacionados a la seguridad y las medidas tomadas para prevenir futuros incidentes.

7) Asegurar que los planes de contingencia son aplicados oportunamente para garantizar la continuidad de las operaciones básicas en caso de que ocurra una emergencia.

8) Asegurar que todo sistema nuevo que se implemente, cumplan con las características de seguridad adecuadas y con las normas establecidas en esta Directiva.

9) Revisar y aprobar los diseños, pruebas de seguridad, certificando los resultados cuando se realiza un cambio en la tecnología, infraestructura y sistemas existentes de hardware y/o software.

10) Efectuar revisiones y auditorias de seguridad periódicamente, en coordinación con la Oficina de Control de Gestión, informando oportunamente a la Alta Dirección sobre los resultados de los mismos.

b. DE LAS DEPENDENCIAS DEL SENAMHI NVOLUCRADAS

1) Cumplir estrictamente las normas establecidas de la presente Directiva.

2) Proteger sus nombres de identificación y códigos de autenticación establecidos. (passwords, números personales de identificación –PIN-y códigos de encriptación).

3) Accesar sólo a las aplicaciones autorizadas y a la información necesaria para realizar sus labores, trabajos y tareas asignadas.

4) Establecer que información que procesan por los medios informáticos de acuerdo a sus labores es sensitiva o confidencial, a fin de darle la mayor seguridad posible.

5) Utilizar los recursos de la institución, solo para fines que benefician únicamente a la Entidad.

6) Brindar apoyo en las revisiones y auditorias de seguridad que le sean solicitadas.

7) Comunicar a la Alta Dirección o a la Oficina de Control de Gestión cualquier trasgresión de las normas establecidas, inmediatamente de conocidas para las correcciones y sanciones que correspondan.

8) Asegurar que los datos y recursos bajo su responsabilidad estén debidamente protegidos con las medidas adecuadas de seguridad.

9) Asegurar que el personal tiene acceso sólo a las aplicaciones y datos necesarios para realizar sus tareas. (Principio del Menor Privilegio).

10) Informar al Administrador de Seguridad de la Oficina General de Estadística e Informática, cualquier cambio en los requerimientos de acceso del personal o cambio relacionado a la seguridad en los sistemas a su cargo, coordinando la existencia de un cambio o transferencia de personal.

11) Revisar la actividad de acceso del personal para asegurar que cumplan con los requerimientos de seguridad y detección de actividad sospechosa, inadecuada o no autorizada.

12) Asegurar que todas las propuestas de adquisición de software, hardware, comunicaciones, aplicaciones y equipos satisfacen los requerimientos de seguridad.

13) Asegurar que el personal de la dependencia conoce y aplica la presente Directiva.

14) Brindar apoyo en las revisiones, inspecciones y auditorias de seguridad que efectúen las Dependencias encargadas de esta labor.

c. DE LA OFICINA DE CONTROL DE GESTION

Verificar oportunamente el cumplimiento de la presente Directiva, informando a la Jefatura del SENAMHI, sobre los resultados de las acciones efectuadas.

El Mayor General FAP
JUAN OVIEDO MOTTA
Jefe del SENAMHI

Distribución.-
Copia: Todas las Dependencias del SENAMHI
Archivo
18.08.05
JAR/WLM/MPH