



PERÚ

Ministerio
de AgriculturaAutoridad Nacional
del Agua

Jefatura

AUTORIDAD NACIONAL DEL AGUA - ANA

NORMAS PARA EL USO CORRECTO DE LOS SISTEMAS DE INFORMACIÓN, SERVICIOS Y RECURSOS INFORMÁTICOS DE LA AUTORIDAD NACIONAL DEL AGUA - ANA

DIRECTIVA GENERAL N° 04 -2011-ANA-J-OSNIRH

Formulada por: Oficina del Sistema Nacional de Información de Recursos Hídricos

Fecha:

I. OBJETIVO

Normar los procesos y mecanismos para el uso de los sistemas de información, servicios y recursos informáticos en la Autoridad Nacional del Agua – ANA.

II. FINALIDAD

Preservar y garantizar la confidencialidad, integridad y disponibilidad de la información en la Autoridad Nacional del Agua – ANA.

III. BASE LEGAL

- Decreto Legislativo N° 997 – Ley de Organización y Funciones del Ministerio de Agricultura.
- Ley N° 29338 – Ley de Recursos Hídricos y su reglamento aprobado por D.S N° 001-2010-AG.
- Ley N° 27309, que incorpora al Código Penal los Delitos Informáticos.
- Ley N° 27269 - Ley de Firmas y Certificados Digitales del Perú
- Ley N° 28493 - Ley que regula el uso del correo electrónico no solicitado (SPAM)
- Ley N° 27291 - Modifica el Código Civil permitiendo la utilización de los medios electrónicos para la comunicación de manifestación de voluntad y la utilización de la firma electrónica.
- Ley N° 27444 - Ley de procedimiento Administrativo General.
- Decreto Supremo N° 006-2010-AG, que aprueba el Reglamento de Organización y Funciones de la ANA.
- Decreto Supremo N° 09-2009-MINAM, que aprueba las Medidas de Ecoeficiencia
- Directiva General N° 0002-2009-ANA-J-OPP - Normas para la Formulación, Trámite, Aprobación y Actualización de Directivas de la Autoridad Nacional del Agua – ANA.

IV. ALCANCE

La presente Directiva es de aplicación en los Órganos de la Sede Central y Órganos Desconcentrados de la Autoridad Nacional del Agua - ANA.

V. NORMAS

5.1. DE LA ORGANIZACIÓN Y GESTIÓN DE LOS SERVICIOS DE LA INFORMATICA DE LA ANA

5.1.1 Gestión de la Informática

La Oficina del Sistema Nacional de Información de Recursos Hídricos (OSNIRH), es responsable de:

- a. La dirección de Tecnologías de Información.- Conjunto de actividades que dan conducción y orientación a la gestión institucional.
- b. El planeamiento estratégico de las Tecnologías de Información.- Consiste en la fijación de objetivos y el desarrollo de los planes necesarios para alcanzarlos. Asimismo, comprende el obtener y combinar de la forma más adecuada los recursos humanos y materiales necesarios para la ejecución de las actividades, con el fin de lograr objetivos a nivel Estratégico Táctico y Operacional.
- c. El apoyo y asesoramiento a los órganos de la Autoridad Nacional del Agua.
- d. La evaluación.- Entendida como el seguimiento de actividades relacionadas con Tecnologías de Información.
- e. El control.- Consistente en el seguimiento del avance del Plan Operativo de Informática, con la finalidad de verificar el cumplimiento de las metas.
- f. La Implementación de las diferentes tecnologías y/o sistemas de información requeridos.

5.1.2 Funciones de Informática

Las funciones de Informática están agrupadas en las áreas siguientes:

- a. **Infraestructura y Seguridad de Tecnologías de Información (TI)**
 - Administrar la plataforma física de servidores (administración experta en sistemas operativos, gestión de actualizaciones y optimización de los mismos).
 - Administrar y asegurar la disponibilidad de las comunicaciones.
 - Mejorar la funcionalidad del software asociado a las comunicaciones e incorporarle novedades.
 - Administrar y asegurar la disponibilidad de los servicios de correo electrónico y mensajería con las que cuente la organización.
 - Mejorar la funcionalidad del software asociado al servicio de correo y mensajería.
 - Administrar la base de datos, que incluye siguiente:
 - i. Recuperar - Crear y probar Respaldos de base de datos.
 - ii. Integridad - Verificar o ayudar a la verificación en la integridad de datos.



- iii. Seguridad - Definir o implementar controles de acceso a los datos.
- iv. Disponibilidad - Asegurarse del mayor tiempo de encendido.
- v. Desempeño - Asegurarse del máximo desempeño incluso con las limitaciones.
- vi. Desarrollo y soporte a pruebas - Ayudar a los programadores e ingenieros a utilizar eficientemente la base de datos.

El diseño lógico y físico de las bases de datos a pesar de no ser obligaciones de un administrador de bases de datos, es a veces parte del trabajo.

- Asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación solo sea posible por las personas que se encuentren acreditadas y dentro de los límites de su autorización.
- Resolver problemáticas como las responsabilidades de la gestión de la seguridad de la información, considerando las regulaciones gubernamentales, la gestión de la disponibilidad, el control de acceso y el análisis de riesgo de las empresas.
- Garantizar la seguridad de todo el sistema informático, minimizando la vulnerabilidad del mismo y detectando tanto riesgos como violaciones, de manera que se logre un servicio de prevención, transparente, confiable, con estricto apego a la ley, salvaguardando la seguridad de la información.

b. Help Desk y Soporte Técnico

- Asistir para resolver problemas con computadoras y productos similares así como los software base de los usuarios de Tecnologías de la Información.
- Brindar un rango de servicios que proporcionan asistencia con el hardware o software de una computadora, o algún otro dispositivo electrónico o mecánico.

c. Desarrollo de Sistemas de Información

- Realizar análisis de sistemas identificando los requerimientos del sistema a desarrollar.
- Generar el diseño arquitectónico y diseño detallado del sistema, basándose en los requisitos.
- Generar prototipos rápidos del sistema (con analistas y programadores) para chequear los requisitos.
- Generar el documento de diseño arquitectónico de software (DDA), y mantenerlo actualizado durante el proyecto.
- Velar porque el producto final se ajuste al diseño realizado (funciones de téster).
- Diseñar Sistemas de información Georreferencial (SIG).
- Realizar la programación de los sistemas luego del análisis y diseño del mismo incluyendo los Sistemas de información Georreferencial (SIG).



- Documentar el desarrollo de un sistema de información, para mantener el estado de los documentos a la par con el estado de desarrollo del sistema.
- Realizar las pruebas respectivas en el desarrollo de sistemas de información (testeo).
- Asegurar la calidad del sistema de información desarrollado.

5.1.3 Plan Estratégico de Tecnologías de Información y Comunicaciones

El Plan Estratégico de Tecnologías de Información y Comunicaciones, es el instrumento de gestión para el desarrollo de las actividades. Este plan contempla los siguientes puntos:

- La Visión Estratégica que se tiene de la ANA, definiendo la misión, objetivos, metas, alineados al planeamiento estratégico de la Institución.
- Las necesidades de información de la Institución y sus dependencias.
- Las directrices técnicas y de gestión que emanan de la Institución.
- El diseño de la Arquitectura de la Información.
- La especificación de los nuevos sistemas, así como una revisión de la situación actual de los Sistemas de Información y definición de las nuevas alternativas tecnológicas.
- Contemplar el diseño de los Planes de Acción, que permitan implementar el Plan Estratégico de Tecnologías de Información y Comunicaciones.

El Plan Estratégico de las Tecnologías de Información y Comunicaciones será revisado periódicamente, a fin de actualizar sus objetivos, metas y alcances.

Las pautas a seguir para evaluar la eficiencia y efectividad de un servicio informático son las siguientes:

Nivel de Eficiencia

Tiempo necesario para el desarrollo de los proyectos informáticos.

Evaluación Costos/Beneficios de las actividades desarrolladas.

Evaluación de la productividad del personal de Informática.

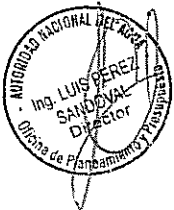
Nivel de Efectividad

Evaluar el nivel de planificación de las actividades, frente a posibles contingencias.

Evaluar la disponibilidad de normas y estándares establecidos.

5.2. DEL HARDWARE Y SOFTWARE

5.2.1 Disposiciones Generales



- a. La instalación y el uso de software no autorizado o adquirido ilegalmente, se consideran como violación a los derechos de autor. En cuanto al software libre, deberá respetarse la propiedad intelectual intrínseca del autor.
- b. Toda dependencia podrá utilizar ÚNICAMENTE el hardware y el software que la OSNIRH haya instalado y oficializado mediante el Acta de Entrega de Equipos de Cómputo (Hardware) y/o Acta de Entrega de Software (Anexos 1 y 2).
- c. El hardware, software y los datos son propiedad de la ANA. Su copia o sustracción o daño intencional será sancionado de acuerdo con las normas y reglamento interno de la Institución.
- d. La OSNIRH llevará el control del hardware y software instalado en los equipos de cómputo de órganos de la ANA.
- e. Periódicamente, la OSNIRH efectuará visitas para verificar el hardware y software utilizado en cada dependencia. Por lo tanto, el detectar hardware y/o software no autorizado, se considerará como una violación a las normas internas de la ANA.
- f. De encontrarse algún hardware y/o software no autorizado por la OSNIRH, esta procederá a desinstalarlo, emitiendo un informe al jefe superior del área por la falta cometida del usuario.
- g. De comprobarse pérdida de datos o deterioro del equipo de cómputo del usuario o daños en la Red-ANA por el uso de hardware y/o software no autorizado, el usuario será sancionado según las normas internas de la Institución.
- h. Todo requerimiento de hardware y/o software adicional debe ser solicitado por escrito a la OSNIRH, utilizando el formato de Informe Técnico Previo de Evaluación de Software y/o Hardware (Anexo 3), a fin que se encargue de evaluar y validar dicha información.
- i. Los dispositivos de almacenamiento que contienen el software original y sus licencias serán administrados y almacenados por la OSNIRH.
- j. La OSNIRH mantendrá actualizado el inventario de equipos de cómputo y software de la ANA, el que se realizará una vez al año como mínimo.
- k. El inventario de hardware debe considerar el detalle de las características técnicas de los componentes de los equipos de cómputo.
- l. El inventario de software debe llegar hasta el nivel del usuario, de tal manera que se identifique el uso de las licencias.
- m. La OSNIRH es la única responsable de autorizar y realizar el traslado e instalación de los diferentes equipos y dispositivos hardware que posee la ANA.
- n. La OSNIRH evaluará y recomendará la actualización del software adquirido cada vez que una nueva versión salga al mercado, a fin de aprovechar las mejoras realizadas a los programas, siempre y cuando se justifique esta actualización.



5.2.2 De la Adquisición de Software y Hardware

- a. De acuerdo con las Políticas Nacionales en Informática y la Legislación vigente, la OSNIRH propiciará la adquisición de los diferentes tipos de licenciamiento de software, para obtener economías de escala y acorde al plan de austeridad del gobierno.
- b. La evaluación de software y hardware se realizará aplicando el formato Informe Técnico Previo de Evaluación de Software y/o Hardware (Anexo 3).
- c. Todo requerimiento, aceptación y/o conformidad de bienes y servicios relacionados con la OSNIRH, deberá contar con el visto bueno del Director de la OSNIRH.
- d. Los trámites para la adquisición de bienes y/o servicios informáticos aprobados por la OSNIRH, así como la adecuación física (de requerirse) de las instalaciones de la Institución serán realizadas por la dependencia respectiva.
- e. La OSNIRH verificará que el uso de sistemas elaborados por servicios de terceros no generen dependencia con los proveedores.

5.2.3 De la Instalación de Software

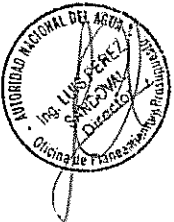
- a. Corresponde a la OSNIRH emitir los procedimientos para la instalación y supervisión del software básico para todos los equipos de cómputo de la Institución.
- b. En los equipos de cómputo, comunicaciones y dispositivos basados en sistemas de cómputo, únicamente se permitirá la instalación de software con licenciamiento apropiado y acorde a la propiedad intelectual.
- c. Toda instalación de software en los equipos de cómputo de la Institución, deberá contar con la aprobación de la OSNIRH, quedando prohibida la instalación de software que no cuente con la licencia correspondiente.
- d. La OSNIRH es la única responsable de brindar asesoría y supervisión en la instalación de software informático y de comunicaciones.
- e. Con el propósito de proteger la integridad de los sistemas informáticos y de comunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad como antivirus y privilegios de acceso, entre otros que se apliquen.

5.2.4 Normas para la Entrega y Control de los Equipos de Cómputo

- a. Todo equipo de cómputo, comunicaciones y software licenciado es parte de los activos de la Institución, los que son cedidos al usuario en uso temporal mientras dure el vínculo laboral entre el trabajador y la ANA.
- b. La ANA asignará al trabajador los recursos informáticos necesarios para la realización de las funciones a través del formulario denominado Acta de Entrega de Equipos de Cómputo (Hardware) y/o Acta de Entrega de Software (Anexos 1 y 2), donde se detallan las características del equipo de cómputo asignado y la relación de programas licenciados para uso del trabajador.



- c. La prueba, instalación y puesta en marcha de los equipos de cómputo y/o dispositivos, serán realizadas por la OSNIRH, quien una vez que compruebe el correcto funcionamiento, oficializará su entrega al área respectiva mediante el Acta de Entrega de Equipos de Cómputo (Hardware) y/o Acta de Entrega de Software (Anexos 1 y 2).
- d. Una vez entregados los equipos de cómputo y/o el software por la OSNIRH, estos serán cargados a la cuenta de activos fijos del respectivo órgano de la ANA y por lo tanto, quedarán bajo su responsabilidad.
- e. Los órganos de la ANA notificarán a la OSNIRH de los cambios de hardware y/o software que realicen.
- f. El usuario es responsable ante las acciones legales que se pudieran tomar en contra de la ANA por la existencia y/o detección no autorizada de cualquier programa o software que no forme parte del Acta de Entrega de Equipos de Cómputo (Hardware) o Acta de Entrega de Software, respectivamente.
- g. El Acta de Entrega de Equipos de Cómputo (Hardware) y/o Acta de Entrega de Software (Anexos 1 y 2) serán actualizadas por la OSNIRH cuando exista una variación a nivel de hardware y/o software de los equipos de cómputo asignados.



5.2.5 Del Software Propiedad de la Institución

- a. Todo software adquirido, sea por compra o donación, es propiedad de la Institución y mantendrá los derechos que la ley de propiedad intelectual le confiera.
- b. La OSNIRH, en coordinación con la Unidad de Control Patrimonial de la Oficina de Administración deberá tener un registro de todo el software licenciado que sea de propiedad de la ANA.
- c. Todos los sistemas informáticos (programas, bases de datos, sistemas operativos, interfaces, y otros) desarrollados con o a través de los recursos de la ANA, se mantendrán como propiedad de la Institución respetando la propiedad intelectual del mismo.
- d. La OSNIRH, en coordinación con la Oficina de Asesoría Jurídica propiciará las acciones correspondientes para registrar la propiedad intelectual de los Sistemas de Información desarrollados por o para la Institución en cumplimiento de las Normas Técnicas de Control y de la Legislación vigente.
- e. La OSNIRH administrará los diferentes tipos de licencias de software y vigilará su vigencia.
- f. Todo el software propiedad de la Institución, deberá ser usado exclusivamente para asuntos relacionados con las actividades de la ANA.

5.2.6 De la Prohibición del Uso de Software sin Licencia

- a. La OSNIRH difundirá periódicamente por medio escrito o charlas de capacitación sobre la prohibición del uso de software sin licencia.
- b. El usuario es el responsable directo de los programas y archivos existentes en el equipo informático asignado.



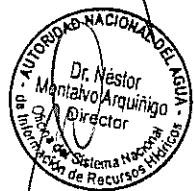
- c. Es responsabilidad de la OSNIRH, la administración del software base y de productividad, evaluar su adquisición y controlar la instalación a los usuarios que lo requieran.
- d. Cualquier software instalado por personal no autorizado y que no cuente con la licencia respectiva, será responsabilidad directa del usuario del equipo frente a situaciones de acciones legales que esta pudiera generar y de las sanciones correspondientes.
- e. El personal encargado del soporte técnico de la OSNIRH es el único autorizado para la instalación y eliminación de programas de base, productividad y/o utilitarios en general.



5.3. PARA EL ALMACENAMIENTO Y RESPALDO DE LA INFORMACIÓN QUE SE PROCESA EN LA ANA

5.3.1 Disposiciones Generales

- a. Debe existir una copia de respaldo de los archivos importantes que están concluidos, tanto en la Sede Central como en una de las sedes de sus órganos desconcentrados, como respaldo preventivo.
- b. La información que se procesa periódicamente, se almacenará por períodos. Entendiéndose por período, al tiempo (mensual, bimensual, trimestral, semestral, o anual) que transcurre para que se ejecute el procesamiento de la información.
- c. Los ambientes donde se depositan los medios magnéticos de respaldo, deben contar con adecuadas condiciones de temperatura y no presentar humedad. La violación de esta norma podrá ser causal de las respectivas sanciones establecidas en el Reglamento de Trabajo y la Legislación vigente.
- d. Los medios magnéticos u ópticos en los cuales se almacena la información histórica deben ser completamente nuevos (primer uso), verificándose su buen estado operacional.
- e. Solo el personal responsable de la seguridad de los archivos tendrá acceso al ambiente donde se encuentren estos medios magnéticos.
- f. El personal encargado de la elaboración de los sistemas de procesamiento de datos, deberá estimar anticipadamente la cantidad necesaria de medios magnéticos u ópticos requeridos para realizar las copias de los archivos de datos y de programas.
- g. El personal que tenga asignado un equipo de cómputo será responsable de realizar las copias de respaldo de su información, de acuerdo a los procedimientos establecidos por la OSNIRH.
- h. El disco duro es un medio de almacenamiento temporal de la información, el cual debe ser depurado permanentemente de los archivos que no volverán a ser utilizados en forma inmediata.



5.4 PARA LA PREVENCIÓN, DETECCIÓN Y ELIMINACIÓN DE VIRUS INFORMÁTICO EN LOS EQUIPOS DE CÓMPUTO DE LA ANA

5.4.1 Disposiciones Generales

- a. La OSNIRH será la responsable de determinar la mejor solución antivirus para la Institución.
- b. Los medios de detección de virus deben ser actualizados permanentemente.
- c. El personal que tiene asignado un equipo de cómputo, deberá encargarse de detectar y eliminar en los medios magnéticos u ópticos, la infección o contagio de virus. A tal efecto, utilizará los procedimientos establecidos por la OSNIRH. Este personal es responsable del control de los medios magnéticos u ópticos venidos del exterior, así como de la posible introducción de virus en el equipo de cómputo.



5.4.2 Disposiciones Específicas

- a. El procedimiento de detección de virus informático debe garantizar que la posible existencia de un virus en un medio magnético u óptico no ingrese directamente al Sistema. Para ello, el programa de detección de virus debe ser instalado en la memoria, a fin que permanentemente se controle cualquier medio de almacenamiento que sea utilizado con el equipo de cómputo.
- b. Para prevenir el contagio de virus en medios magnéticos se deberá considerar lo siguiente:
 - Nunca se deben ejecutar programas de origen desconocido.
 - Efectuar periódicamente la depuración de archivos en los discos duros de la computadora.
- c. Se consideran medios de infección por virus a los siguientes:
 - Un medio magnético u óptico.
 - A través de la adquisición o movimiento de máquinas infectadas a la ANA.
 - A través de la Red de datos.
 - Correo electrónico.
 - Internet.
- d. Los antivirus de la Institución, para servidores y estaciones de trabajo, deben activarse de tal forma que se verifiquen todos los archivos, aun los que se encuentren compactados, y la acción por defecto a seguir será la de eliminar el virus automáticamente.
- e. Los servidores de correo deben contar con antivirus para correo. Si el mensaje que detecta contiene un virus o "troyano" - "caballo de Troya" que no puede ser removido, debe eliminarse el mensaje inmediatamente. Asimismo, se deberá informar al destinatario de correo, el nombre del remitente y que su mensaje fue borrado por contener virus.



5.5 PARA LA SEGURIDAD E INTEGRIDAD DE LA INFORMACIÓN QUE SE PROCESA EN LA ANA

5.5.1 Disposiciones Generales

- a. Toda computadora será entregada por la OSNIRH con los privilegios necesarios para el correcto funcionamiento del equipo. Estos privilegios deberán restringir la instalación de software.
- b. El usuario firmará un compromiso para mantener en secreto sus contraseñas personales y/o las compartidas por un grupo solo entre los miembros de ese grupo.



- c. El usuario solicitará el cambio de contraseñas cuando se tenga algún indicio de su vulnerabilidad.
- d. La OSNIRH no se responsabiliza de pérdida de información por negligencia del usuario o cambio de clave sin previa coordinación.
- e. Queda estrictamente prohibido otorgar acceso al equipo asignado a personas externas a la ANA.
- f. Es responsabilidad del usuario, bajo supervisión de su jefe inmediato superior, llevar un control de toda la información que este procese.
- g. Para el ingreso al centro de cómputo se debe contar con la autorización de la OSNIRH, registrando el ingreso y salida del área.
- h. La OSNIRH adoptará las medidas de seguridad, que garanticen el cumplimiento de las presentes normas.
- i. Los usuarios evitarán exponer sus contraseñas al acceso de terceros. El usuario de los sistemas de información que disponga de una contraseña, será responsable del mal uso que pudiera darse por personas no autorizadas.



5.5.2 De los Sistemas de Información

- a. En los Sistemas Informáticos es obligatorio utilizar procesos que cuenten con rutinas de control para el acceso de los usuarios con su correspondiente nivel de acceso, el cual incluye la lectura o modificación en sus diferentes formas.
- b. Como mínimo deben existir tres niveles de acceso a la información: consultas, mantenimientos y reportes. Para garantizar estos niveles, cada palabra clave tendrá asignada uno de estos niveles de acceso.
- c. La información que se considere restringida o reservada estará debidamente identificada, así como los usuarios que accedan a ella.
- d. Los usuarios de la información restringida o reservada realizarán estrictamente lo indicado en cada procedimiento establecido de procesamiento de la información, para lo cual estos deberán estar claramente documentados.
- e. Cada área de la ANA, para la seguridad de la información, deberá designar un responsable para el control y distribución de la información.
- f. Los Sistemas de Gestión de Base de Datos, deben brindar facilidades para su restauración; es decir, poder realizarse con rapidez y con la mínima pérdida de información.
- g. En caso de dejar su puesto de trabajo, el usuario deberá salir del sistema al que ha ingresado para evitar el acceso de personas no autorizadas a utilizar su cuenta aperturada. En caso que el sistema siga procesando información, deberá iniciar el protector de pantalla con contraseña.
- h. Las sesiones realizadas satisfactoriamente al inicio de la sesión, deben indicar la hora y fecha de inicio, así como la hora y fecha de su finalización.

- i. La identificación del usuario y la clave de acceso serán suspendidas después de un período sin uso máximo de treinta (30) días, siendo responsable el encargado de la seguridad de la OSNIRH verificar su cumplimiento.

5.5.3 Protección de la Comunicación Remota Frente a Intervención de Intrusos

- a. El encargado de la Administración de la Red y Comunicaciones de la ANA, debe establecer los mecanismos para implementar autenticación encriptada en el servidor y en todos los usuarios externos de la ANA desde el inicio de la sesión.
- b. El encargado de la Administración de la Red y Comunicaciones de la ANA debe conceder capacidad de acceso remoto solo a aquellos usuarios que lo requieran en horario preestablecido.



5.5.4 Para mantener la Información de Acceso Remoto en Forma Confidencial

- a. La OSNIRH será la encargada de mantener en forma confidencial toda la información referente al acceso a las computadoras y sistemas de comunicación. Esta información, sin excepción, no será publicada ni listada en directorios ni tarjetas de presentación. Dicha información no será entregada a terceros, a menos que se disponga de la respectiva autorización otorgada por la OSNIRH.
- b. El encargado de la Administración de la Red y Comunicaciones de la ANA periódicamente verificará y monitoreará el acceso remoto al Sistema de Comunicaciones, con el fin de identificar a los usuarios que están accedendo frecuentemente y velar porque el sistema sea seguro. Deberá establecer mecanismos de ataque a su propia red, a fin de confirmar su seguridad.



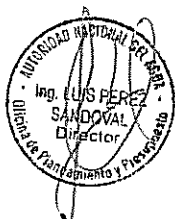
5.5.5 De la Verificación Periódica de los Cambios de Contraseñas y Registros (Logs) de Seguridad de los Accesos Remotos

- a. El encargado de Administración de la Red y Comunicaciones de la ANA cambiará las contraseñas periódicamente a los usuarios externos de la ANA que utilicen el servicio de acceso remoto.
- b. Se deberá verificar con prontitud los permisos de accesos remotos que ya no estén activos y en los casos de usuarios externos de la ANA que ya no existan o no estén autorizados.
- c. Se deberá periódicamente monitorear el registro (Logs) de acceso remoto, a fin de identificar intentos de intrusión a la red de comunicaciones.



5.5.6 Del Control de Acceso al Equipo de Cómputo

- a. Los equipos de cómputo son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.
- b. Las áreas donde se encuentre equipo cuyo propósito reúna características de imprescindible y/o de misión crítica, deberán sujetarse a las normas que establezca la OSNIRH de la ANA.



5.5.7 Del Control de Acceso Local y Remoto a la Red-ANA



- a. El encargado de la Administración de la Red y Comunicaciones de la ANA es responsable de proporcionar a los usuarios el acceso local y remoto a los recursos informáticos.
- b. Dado el carácter unipersonal del acceso a la Red-ANA, la OSNIRH verificará el uso responsable, de acuerdo a las normas establecidas para el uso de la Red-ANA.
- c. El acceso físico y lógico a equipos especializados de cómputo - servidores, enrutadores, bases de datos, equipos de cómputo centralizados y distribuidos y otros - conectados a la Red-ANA son administrados por la OSNIRH.
- d. Todo equipo de cómputo que esté o sea conectado a la Red-ANA, o aquellas que en forma autónoma se tengan y que sean propiedad de la Institución, debe sujetarse a los procedimientos de acceso que emite la OSNIRH.
- e. En caso se requiera el acceso de terceros a los servidores o equipos de cómputo de la Red-ANA, este deberá ser autorizado por la OSNIRH. El usuario de estos servicios deberá sujetarse a las normas de uso de la Red-ANA.



5.5.8 Del Acceso a los Sistemas de Información

- a. Tendrán acceso a los Sistemas de Información, solo aquellos usuarios de la Red-ANA autorizados por el jefe de mayor jerarquía del órgano correspondiente.
- b. La instalación y uso de los sistemas de información se rigen por las presentes normas de uso de la Red-ANA.



5.5.9 De los Controles de Acceso

- a. Todo acceso lógico a cualquier recurso de la Red-ANA contará con un mecanismo de autenticación de usuarios, que permita identificarlos y en el que se pueda aplicar las reglas de acceso a los recursos asociados.
- b. El acceso a los servidores será restringido de acuerdo a las necesidades de los usuarios, lo cual será controlado por la OSNIRH en coordinación con los responsables de los órganos de los usuarios respectivos.
- c. La OSNIRH será responsable de configurar correctamente el equipo de cómputo que se le asigne a un usuario, de manera que garantice la seguridad de la información contenida en ella.



5.5.10 De los Registros Vitales

- a. La información vital es aquella que ante una alteración y/o destrucción no autorizada, tenga como consecuencia perjuicios económicos y/u operativos a la Institución.
- b. La determinación de la información vital será definida por la OSNIRH en coordinación con las áreas usuarias.
- c. La información vital de la Institución y su respectivo procesamiento, está considerada como de alta prioridad dentro de los planes de desarrollo,



cronograma de respaldo de la información (backup) y los planes de contingencia de la ANA.

- d. Periódicamente, la OSNIRH supervisará el cumplimiento del proceso de resguardo de la información vital de la Institución y determinará las acciones correctivas cuando encuentre que no se está cumpliendo con las políticas de resguardo de la información.

5.5.11 Del Pase a Producción

- a. Todo trabajo de desarrollo de aplicativos que haya sido culminado, probado, documentado y aprobado por el área usuaria propietaria de la información, pasará del ambiente de desarrollo al ambiente de producción para su uso correspondiente.
- b. Todo pase al ambiente de producción, deberá efectuarse con los controles que garanticen la administración adecuada de los códigos fuentes y los códigos objetos y previa aprobación por parte de la OSNIRH.
- c. El control del pase a producción, deberá ser administrado por el responsable de desarrollo de la OSNIRH, emitiéndose una certificación de la ejecución de la solicitud.

5.5.12 De los Servidores de Respaldo

- a. Los servidores institucionales deberán contar con una configuración de respaldo que garantice la continuidad de las operaciones, aun a pesar de las fallas que puedan producirse en estos.
- b. La configuración de respaldo de los servidores institucionales deben considerar criterios tolerantes a fallas:
 - Sistemas de alimentación redundantes.
 - Sistemas de respaldo eléctrico (UPS, Grupo Electrónico).
 - Respaldo alterno para las comunicaciones.
 - Respaldo de la base de datos en línea.
 - Protección de discos.
 - Clustering de servidores o replicación de datos en ambiente alterno.

5.5.13 Para la Administración de Cuentas de Usuario y Claves de Acceso (Password)

- a. La identificación de los usuarios (cuenta de usuario) y las contraseñas (passwords) deben ser únicas para cada usuario autorizado.
- b. La convención de nombres para la determinación de cuentas de usuario será la primera letra del nombre y el apellido paterno. De repetirse el nombre de cuenta, deberá agregarse un carácter que lo diferencie como puede ser la inicial de su segundo apellido.
- c. Todas las formas de contraseñas de accesos a cualquier recurso de la Red-ANA tiene carácter personal y es intransferible, por lo que ningún usuario deberá compartir sus contraseñas.
- d. La OSNIRH definirá las contraseñas de acceso de acuerdo a las políticas y normas establecidas.

- e. La Unidad de Recursos Humanos debe comunicar a la OSNIRH la relación de personas que hayan ingresado a laborar y de las que han dejado de hacerlo, para la activación o desactivación de las cuentas de usuarios respectivas.

5.5.14 De la Determinación de las Contraseñas

- a. La longitud de contraseñas debe tener por lo menos ocho (8) caracteres, incluyendo letras y números. Nunca debe usarse exclusivamente números.
- b. Los usuarios no deben escoger contraseñas que estén relacionadas o que evidencien datos personales, como su nombre, iniciales, fecha de natalicio, ni similares que puedan ser determinadas fácilmente. Esto significa que las contraseñas no deben ser relativas a la labor del usuario o su vida personal.
- c. Para impedir que una contraseña pueda ser descifrada, se limitará el número de intentos consecutivos a tres (3) intentos de fracaso, luego del cual el ingreso al sistema será suspendido hasta que sea reinicializado por el administrador del sistema respectivo.
- d. La OSNIRH deshabilitará a los usuarios y contraseñas que vengan por defecto con la instalación de los sistemas operativos, bases de datos y software al que sea aplicable.



5.5.15 Del Cambio de Contraseñas

- a. Las contraseñas deben forzarse a ser cambiadas automáticamente una vez cada 90 días.
- b. En caso el usuario no realice el cambio de clave, el personal a cargo de la seguridad de la OSNIRH enviará un mensaje al usuario para que efectúe el cambio. En caso de no realizarlo, el usuario no podrá ingresar al sistema.



5.5.16 Para el Establecimiento de Cuentas de Administración de los Servicios de Red

- a. Las claves de los servicios de red serán registradas y almacenadas en un lugar seguro, donde solo tenga acceso el personal autorizado por la OSNIRH.
- b. La cuenta administrador no deberá ser compartida y se deberá crear una cuenta personal para el trabajador a cargo de la misma, destinada solamente para las actividades que no estén relacionadas con la función de administrador.
- c. Ante el cese de labores de un administrador, con antelación ó inmediatamente, deberá cambiarse la contraseña de la cuenta en prevención de la seguridad del Sistema de Información.
- d. Se deberá cambiar el password de la cuenta administrador, en prevención de la seguridad del sistema de comunicación, si se sospecha que el password de administrador ha sido revelado.
- e. Se cambiará el nombre de usuario de la cuenta administrador para una mayor protección en caso de un ataque de intrusos.



- f. Se mantendrá un mínimo de cuentas con derechos de Administrador para tener un menor riesgo de accesos peligrosos a la red.

5.5.17 Para la Utilización de Cuentas de Administración de los Servicios de Red



- a. El administrador de red y el administrador de bases de datos de la Red-ANA deben iniciar una sesión solo cuando sea necesario, dentro del marco de sus funciones operativas.
- b. El administrador de red y el administrador de bases de datos de la Red-ANA nunca deben ejecutar en sus actividades diarias, trabajos personales (lecturas de su e-mail, navegar por el Internet, escribir sus reportes semanales) cuando hayan iniciado una sesión con su cuenta de Administrador.
- c. El administrador de red y el administrador de bases de datos de la Red-ANA deben usar siempre protectores de pantalla como medida de protección de las operaciones que están realizando.



- d. El administrador de red y el administrador de bases de datos de la Red-ANA deben ser instruidos en "ataques de intrusos", con el fin de poder tomar las medidas técnicas necesarias frente a una amenaza de intrusión.



- e. Para máxima seguridad, el administrador de red y el administrador de bases de datos de la Red-ANA deben trabajar en computadoras dedicadas para la administración de la red en forma remota. Generalmente, estas computadoras deben ser estrictamente controladas asignando derechos de ingreso local solo para administradores autorizados.

- f. Las computadoras para la administración de la red deben tener solamente las herramientas administrativas necesarias y no aplicaciones de uso general (procesadores de texto, navegadores y otros). Estas computadoras que tienen software de administración instalado deben estar en un área protegida (centro de cómputo).

5.5.18 Para el Uso de los Recursos Compartidos



- a. Los usuarios de los equipos de cómputo deberán minimizar estrictamente el número de directorios compartidos y los permisos otorgados.
- b. El nombre que hace referencia al directorio compartido no debe dar información alguna de la información contenida en él.
- c. No se debe compartir el directorio raíz, a fin de evitar que se visualicen las distintas carpetas compartidas.

5.5.19 De la Confidencialidad de la Información en Medios de Almacenamiento



- a. Los responsables de los órganos de la ANA son los únicos facultados a autorizar la divulgación de información interna, de acuerdo a la clasificación de la referida información.



- b. El acceso a la información confidencial debe ser restringido a usuarios autorizados, siendo los usuarios propietarios de dicha información quienes determinarán las autorizaciones.
- c. Los trabajadores de la ANA son responsables de la confidencialidad de la información a la que tienen acceso como parte de sus labores, no pudiendo difundirla por ningún medio sin la autorización de las instancias respectivas. La violación de esta norma será causal de las respectivas sanciones establecidas en el Reglamento de Trabajo y la Legislación vigente.
- d. Las especificaciones técnicas de los Sistemas de Información (Especificaciones de producto, base de datos, lista de direcciones, programas de computación, documentación y otros) deben ser utilizadas solo para los fines de gestión. El uso de esta información para cualquier otra razón solo se permitirá con permiso escrito del responsable del órgano propietario de la información.
- e. Los Sistemas de Información no deben divulgar los nombres, direcciones, números de teléfono privados y demás datos personales de los usuarios, a menos que sean requeridos para propósitos de la Institución. Las excepciones se harán cuando la divulgación sea requerida por la Ley o cuando las personas implicadas hayan consentido anteriormente su divulgación.



5.6 PARA LA PROTECCIÓN FÍSICA DE LOS EQUIPOS Y MEDIOS DE PROCESAMIENTO DE LA INFORMACIÓN DE LA ANA

5.6.1 Referente a las Instalaciones Eléctricas

- a. La Institución debe contar con una red eléctrica independiente para los equipos de cómputo.
- b. La Institución debe contar con un sistema de pozos de tierra eléctrico para los equipos de cómputo que asegure su adecuado funcionamiento.
- c. Realizar periódicamente mediciones de la carga eléctrica, asegurando que sea la adecuada y requerida en la Red Eléctrica de Cómputo.
- d. Asegurar un suministro de energía eléctrica de voltaje estable con la ayuda de sistemas de estabilización de voltaje, supresores de picos y unidades de potencia contra cortes de fluidos (UPS).
- e. Todo el cableado eléctrico deberá estar debidamente aislado y protegido dentro de tubos y/o canaletas de PVC, que cumplan con las normas técnicas establecidas para este tipo de cableado.
- f. Por cada pabellón y/o piso se debe establecer tableros de distribución eléctrica para los equipos de cómputo.

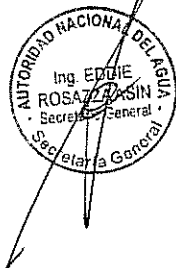


5.6.2 Referente a las Instalaciones de Aire Acondicionado

- a. Ningún equipo de aire acondicionado deberá ser conectado a la Red Eléctrica de Cómputo.
- b. Los equipos de aire acondicionado no deben ser instalados próximos a materiales inflamables.



5.6.3 Disposiciones Complementarias



- a. Queda terminantemente prohibido conectar artefactos eléctricos a la Red Eléctrica de Cómputo.
- b. Los equipos de cómputo no deberán permanecer encendidos si no están siendo utilizados.
- c. La ANA deberá contar con extintores adecuados para combatir los incendios producidos por equipos eléctricos y/o electrónicos.
- d. Se recomienda que los sistemas de agua y desagüe se encuentren a niveles inferiores al Centro de Cómputo.
- e. Queda terminantemente prohibido ingerir alimentos y bebidas cerca a los equipos de cómputo.



5.7 PARA LA ELABORACIÓN E IMPLEMENTACIÓN DE SISTEMAS DE INFORMACIÓN EN LA ANA

5.7.1 De la Elaboración de los Sistemas de Información

- a. La OSNIRH deberá establecer los estándares de desarrollo que garanticen la interpretación adecuada de los códigos fuentes e incorporen las políticas y normas de seguridad.
- b. El diseño y desarrollo de sistemas, se deberá llevar a cabo conforme a los objetivos establecidos, considerando evaluar el volumen de información a procesar, áreas de almacenamiento de información, tiempos de respuesta requeridos, factibilidad para la programación, integridad de los datos, el uso que se dará a la información procesada y su posible concurrencia con otras áreas que requieran sus resultados como insumo.
- c. La elaboración de Sistemas de Información deberá cumplir con los puntos especificados para el desarrollo y documentación conforme a la Norma ISO IEC/12207: Proceso del Ciclo de vida del Software.
- d. Los sistemas existentes, así como los de nueva creación, deberán considerar en su algoritmo de programación y de acuerdo al estándar internacional ISO 8601 (aaaa-mm-dd), el manejo de cuatro (4) dígitos para referirse al año, en los procesos que involucren la representación de fecha en formato numérico.
- e. Los operarios de los sistemas implementados, no podrán realizar ninguna modificación a estos.
- f. Los sistemas de información de la ANA serán clasificados en relación a su importancia como:
 - Sistemas Estratégicos: los que automatizan procesos y/o actividades que permitan cumplir las funciones de los órganos de línea para las que han sido creadas.
 - Sistemas de Información Gerencial: los que van a servir para la toma de decisiones, consolidan y resumen las transacciones que están en marcha dentro de la ANA.
 - Sistemas de Soporte: son generalmente operativos, de tipo administrativo, haciendo más eficiente el funcionamiento interno de la ANA.



5.7.2 Del Control de Calidad para las Aplicaciones

- a. Todo cambio realizado en los códigos fuentes deberá pasar obligatoriamente por un periodo de pruebas, que garantice el correcto funcionamiento del mismo de acuerdo a las normas vigentes.
- b. Todas las pruebas que se realicen deberán contar con la participación del área usuaria, para lo cual se establecerá un cronograma.
- c. Las pruebas deberán hacerse con datos que consideren todos los casos existentes para un determinado aplicativo, módulo y/o funcionalidad.
- d. Por ningún motivo se harán pruebas directamente con los datos del servidor de producción.
- e. Las consideraciones para evaluar la aplicación son las siguientes:
 - Validación de la información, de entrada y de salida.
 - Verificación de los niveles de seguridad.
 - Resultado de procesos de consulta.
 - Resultado de procesos de cálculo.
 - Tiempo de respuesta de procesamiento y recuperación de datos.
 - Facilidad de uso.
 - Revisión de auditoría de transacciones a registros sensibles.
 - Portabilidad del Sistema.



5.7.3 Para el Control de las Aplicaciones que pasan de Desarrollo a Producción

- a. La información residente en la base de datos de producción es de propiedad de la ANA, debiendo realizarse los accesos solo mediante aplicativos debidamente registrados y con los controles necesarios.
- b. La OSNIRH es responsable de implementar los procedimientos formales para el pase a producción, que garanticen la correspondencia entre los códigos fuente y base de datos de prueba y el ambiente de producción.
- c. Todo proyecto que culmine en el desarrollo o modificación de un sistema de información debe tener un pase formal a producción, una vez que se haya cumplido con lo indicado en la norma de control de calidad de las aplicaciones.
- d. Realizado el pase a producción, el área de desarrollo es responsable de la seguridad y administración del código fuente.
- e. Toda solicitud de baja de aplicaciones deberá contar con la aprobación del área usuaria.
- f. En la implantación de los sistemas, el área usuaria deberá prever en coordinación con la OSNIRH la capacitación del personal necesario para su operación.
- g. Queda prohibida la reproducción de los sistemas que hayan sido instalados en las áreas usuarias.

5.8 PARA LAS COMUNICACIONES, USO DE INTERNET Y CORREO ELECTRÓNICO EN LA ANA

5.8.1 Disposiciones Generales

- a. El correo electrónico institucional es una herramienta de comunicación e intercambio de información oficial entre personas e instituciones; no es una herramienta de difusión indiscriminada de información, con la excepción de las listas de interés configuradas y/o establecidas por la OSNIRH.
- b. Las notificaciones institucionales pueden efectuarse mediante correo electrónico conforme al numeral 20.1.2 del artículo 20° de la Ley N° 27444 - Ley del Procedimiento Administrativo General.
- c. La OSNIRH es la responsable de capacitar al personal en el uso del correo electrónico institucional.
- d. Los usuarios de las cuentas de correo electrónico institucional se comprometen y obligan a aceptar las normas establecidas por la Institución y a someterse a ellas, por lo que son responsables de todas las actividades que se realicen con sus respectivas cuentas.
- e. Las cuentas de correo electrónico otorgadas por la ANA, deben usarse para actividades que estén relacionadas con el cumplimiento de su función en la Institución.
- f. El nombre de la cuenta de correo electrónico institucional estará conformado por la letra inicial del nombre de pila del usuario seguido inmediatamente del apellido paterno, ligado con el símbolo @ al nombre de dominio de la Institución.
- g. En caso de existir dos construcciones similares, el Administrador de Correo Electrónico en coordinación con las personas involucradas, acordarán el nombre de la cuenta tratando de seguir la regla aquí definida.
- h. La ANA garantizará la privacidad de las cuentas de correo electrónico institucional de todos los usuarios.



5.8.2 De la Creación, Modificación y Bajas de las Cuentas de Correo Electrónico y Acceso a Internet

- a. Toda persona que labore en la ANA, según corresponda, contará con una cuenta de correo electrónico institucional y acceso a Internet.
- b. La Unidad de Recursos Humanos de la ANA, periódicamente remitirá a la OSNIRH, la relación de personas que laboren o presten servicios a la Institución y que requieran de una cuenta de correo electrónico y acceso a Internet para el desarrollo de sus funciones.
- c. La Unidad de Recursos Humanos remitirá mensualmente a la OSNIRH la relación de personas cuyo vínculo laboral, en cualquier modalidad, haya cesado con la Institución, a fin de eliminar la cuenta de correo electrónico y acceso a Internet respectiva.
- d. El usuario podrá solicitar mediante un mensaje de correo electrónico dirigido al Administrador de Correo Electrónico de la ANA, la modificación de los datos suministrados para la creación de la cuenta. En ningún caso se podrá usar esta información para la creación de una nueva cuenta de correo electrónico.



5.8.3 Del Buen Uso del Correo Electrónico

- a. Uso de Contraseñas



- La OSNIRH otorgará a los usuarios que tienen asignada una cuenta de correo electrónico institucional una contraseña de acceso, la cual debe mantener en secreto para que su cuenta de correo no pueda ser utilizada por otra persona.
- Cuando el usuario deje de usar su estación de trabajo deberá cerrar el software de correo electrónico, para evitar que otra persona use su cuenta de correo.
- Todo protector de pantalla deberá ser configurado activando su respectiva contraseña.

b. Lectura de Correo Electrónico



- Los usuarios de la Sede Central que tienen asignada una cuenta de correo electrónico institucional, deben mantener activo el software de correo electrónico y activada la opción de aviso de recepción cuando llegue un nuevo mensaje. Los usuarios de los órganos desconcentrados deberán conectarse al correo electrónico con la mayor frecuencia posible para leer sus mensajes.
- Se deben eliminar permanentemente los mensajes de correo y/o adjuntos que sean innecesarios.
- Los mensajes de correo electrónico que se deseen conservar, deberán ser agrupados por temas en carpetas personales.
- Al recibir un mensaje de correo electrónico que se considere ofensivo, se debe reenviar el mensaje hacia el Administrador de Correo Electrónico de la OSNIRH de la ANA, con el fin de que se puedan tomar las acciones respectivas.



c. Envío de Correo Electrónico



- Utilizar siempre el campo "asunto" a fin de resumir el tema del mensaje.
- Expresar las ideas completas, con las palabras y signos de puntuación adecuados en el cuerpo del mensaje.
- Enviar mensajes bien formateados y evitar el uso generalizado de letras mayúsculas.
- No utilizar tabuladores, ya que existen software administradores de correo que no reconocen este tipo de caracteres, lo que puede introducir caracteres no válidos en el mensaje a recibirse.
- Antes de enviar el mensaje, revisar el texto que lo compone y los destinatarios, con el fin de corregir posibles errores de ortografía, forma o fondo.



d. Reenvío de Mensajes



- Para el reenvío de un mensaje, incluir el mensaje original, para que el destinatario conozca el contexto en que se está dando el mensaje que recibe. No incluir ningún archivo adjunto que se pueda haber recibido originalmente, a no ser que se haya realizado modificaciones al(los) archivo(s).

e. Autofirmas



- La firma debe ser breve e informativa.
- No incluir la dirección de correo electrónico en la firma, porque esta ya fue incluida de manera automática en la parte superior del mensaje.

f. Tamaño de los Mensajes

- La OSNIRH determinará el tamaño máximo que deben tener los mensajes del correo electrónico institucional.
- Es obligación de los usuarios depurar su buzón de correo electrónico periódicamente.
- Los archivos adjuntos que se consideren importantes deberán ser almacenados localmente en las unidades de disco del equipo de cómputo del usuario.

g. Vigencia de los Mensajes

- La OSNIRH notificará a los usuarios cuyo buzón se encuentre al 80% de su capacidad límite, a fin que este proceda a su depuración.
- Los buzones de correo electrónico que hayan llegado al límite establecido por la OSNIRH, serán depurados automáticamente, eliminándose los mensajes de correo y/o archivos adjuntos que tengan una antigüedad mayor a 30 días, contados desde la fecha de entrega o recepción de los mismos.



5.8.4 Del Mal Uso del Correo Electrónico

- a. Está estrictamente prohibido facilitar u ofrecer la cuenta y/o buzón del correo electrónico institucional a terceras personas.
- b. Se considera como mal uso del correo electrónico institucional realizar las siguientes actividades:
- Utilizar el correo electrónico institucional para cualquier propósito comercial o financiero ajeno a la Institución.
 - Participar en la propagación de mensajes encadenados o participar en esquemas piramidales o similares.
 - Distribuir mensajes con contenidos impropios y/o lesivos a la moral.
 - Falsificar las cuentas de correo electrónico.
 - Utilizar el correo electrónico institucional para recoger los mensajes de correos de otro proveedor de Internet.
- c. Se penalizará con la cancelación de la cuenta de correo electrónico, el envío de mensajes a foros de discusión (listas de distribución y/o newsgroups) que comprometan la información de la Institución o violen las leyes del Estado Peruano, sin perjuicio de poder ser sujeto de otras sanciones y/o penalidades derivadas de tal actividad.
- d. Se considera, adicionalmente, malas prácticas en el uso de correo electrónico:
- Difusión de contenido inadecuado.
 - i. Son considerados contenidos inadecuados todo lo que constituya complicidad con hechos delictivos, por ejemplo: apología del terrorismo, uso y/o distribución de programas piratas, todo tipo de pornografía, amenazas, estafas, esquemas de enriquecimiento piramidal, virus o código hostil en general.
 - ii. Contenido fuera de contexto en un foro temático.
 - Difusión masiva no autorizada.



iii. Enviar de forma masiva publicidad o cualquier otro tipo de correo no solicitado, "spam".

• Ataques con objeto de imposibilitar o dificultar el servicio, "mail bombing".

iv. Dirigir a un usuario o al propio sistema de correo electrónico, mensajes que tengan el objetivo de paralizar el servicio por saturación de las líneas, de la capacidad del servidor de correo, o del espacio en disco del usuario.

v. Suscripción indiscriminada a listas de correo.

5.8.5 Del Uso del Acceso a Internet

a. La ANA proporciona las herramientas de acceso a Internet a sus trabajadores y servidores, con la finalidad de que realicen actividades que estén relacionadas con sus labores y responsabilidades.

b. El usuario de la ANA con acceso a Internet debe aplicar su buen criterio para un uso racional de esta tecnología, que no ocasione un abuso de esta herramienta en desmedro de su productividad y responsabilidades.

c. El usuario con acceso a Internet debe ser consciente de la navegación por sitios dudosos o de origen desconocido y riesgoso, así como la descarga de archivos o documentos de estos sitios.

d. Se encuentran prohibidas las siguientes actividades a través del uso de Internet:

- El acceso a sitios web que contengan material pornográfico o cualquier otro similar que muestre contenidos para adultos.
- El acceso a sitios web que ofrezcan software ilegal o comúnmente denominados pirata, números de serie de software comercial, o cualquier otro similar que vaya contra los derechos de autor.
- Descargar archivos ejecutables (.exe, .dll, .bat, .com, .vbs) debido a que su uso puede exponer a toda la red de la Institución a infecciones de virus. Cualquier descarga de este tipo deberá ser aprobada y coordinada con la OSNIRH de la ANA.
- Descargar archivos de gran tamaño (mayores de 50 MB) durante las horas de trabajo, debido a que degrada considerablemente la performance de la red (el ancho de banda). Cualquier descarga de este tipo deberá ser programada para ser ejecutada fuera de las horas de trabajo y con la aprobación de la OSNIRH de la ANA.
- Escuchar y/o ver en línea desde Internet, audio (música, radio y otros) y videos (películas, televisión y otros), dado que esto provoca la saturación del ancho de banda de acceso a Internet institucional.
- Descargar archivos de música y/o videos que atenten contra los derechos de autor.
- El acceso a Internet para uso recreacional a través de las redes de la Institución está prohibido. El usuario es el responsable de hacer cumplir esta política.

5.8.6 De las Prioridades del Tráfico de Red

a. El Administrador de Red de la ANA deberá realizar un análisis detallado del tráfico en la red, determinando todos los protocolos y procesos que circulan, midiendo con esto la capacidad del ancho de banda que se requiere para el funcionamiento óptimo de la red de comunicaciones.



- b. La OSNIRH debe determinar los procesos más críticos y de información sensible para asignarle una mayor prioridad de tráfico en la red de comunicaciones.
- c. El Administrador de la Red debe monitorear continuamente las estadísticas de los equipos de comunicación, a fin de determinar la performance de la red, lo que indicará si el crecimiento en equipos y ancho de banda es el adecuado o necesitará implementarse con más equipo.

5.9 DEL SOPORTE TÉCNICO A LOS EQUIPOS DE CÓMPUTO

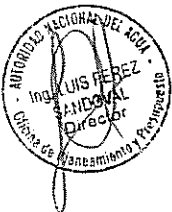
5.9.1 De la Atención a los Usuarios

- a. La OSNIRH brindará la asistencia técnica al usuario a través del servicio de Help Desk.
- b. Los usuarios registrarán su solicitud de asistencia técnica al Help Desk, a fin de reportar los problemas que pudieran ocurrir como resultado del uso de los equipos de cómputo y de los programas existentes en él.
- c. El Help Desk emitirá una Ficha de Atención Técnica (Anexo 4) en la que se registrará el problema reportado y los datos generales del usuario.
- d. Al término de la atención, el técnico encargado completará la Ficha de Atención Técnica (Anexo 4) con las acciones realizadas, dando su conformidad el usuario mediante su firma en la Ficha de Atención.
- e. En el caso que sea necesaria la adquisición de repuestos o el servicio de una empresa especializada, la OSNIRH elaborará el informe técnico respectivo sobre el particular, para la ejecución por parte del área solicitante. Una vez adquiridos los repuestos o concluido el servicio de terceros, la OSNIRH procederá a la instalación o verificación de lo solicitado.



5.9.2 De la Instalación del Equipo de Cómputo

- a. Todo equipo de cómputo (computadoras, servidores, laptops y periféricos), que esté o sea conectado a la Red-ANA, o aquel que en forma autónoma se tenga y que sea propiedad de la Institución, debe sujetarse a las normas y procedimientos de instalación que emita la OSNIRH de la ANA.
- b. Los equipos de cómputo de la Institución que sean de propósito específico y tengan una misión crítica asignada, requieren estar ubicados en un área que cumpla con los requerimientos de: seguridad física, condiciones ambientales y de alimentación eléctrica adecuadas para su propósito.



5.9.3 Del Mantenimiento de los Equipos de Cómputo

- a. La OSNIRH es la encargada de realizar el mantenimiento preventivo y/o correctivo de los equipos de cómputo, la conservación de su instalación, la verificación de la seguridad física y su acondicionamiento específico a que tenga lugar.
- b. En el caso de los equipos de cómputo atendidos por terceros, la OSNIRH deberá supervisar y dar su conformidad y aceptación del servicio prestado.



- c. Los órganos desconcentrados de la ANA pueden realizar el mantenimiento preventivo y correctivo a sus equipos de cómputo, a partir del momento que sean autorizados por la OSNIRH.
- d. La OSNIRH dará a conocer la relación de técnicos autorizados a brindar el servicio de soporte técnico en la Institución.
- e. La OSNIRH programará y difundirá las fechas en las que se realizará el mantenimiento preventivo a los equipos de cómputo de la Sede Central, estando obligadas las áreas de la Institución a dar las facilidades correspondientes para el desarrollo de esta actividad.
- f. Queda estrictamente prohibido dar mantenimiento preventivo y/o correctivo a equipos de cómputo que no sean propiedad de la ANA.



5.9.4 De la Actualización de los Equipos de Cómputo

- a. La OSNIRH es la única responsable de realizar el diagnóstico de actualización de los equipos de cómputo y comunicaciones de la Institución.
- b. El acceso a cambios en la configuración de los equipos, a la apertura y cambio de dispositivos o accesorios; asimismo, cualquier acción que constituya alteración del hardware y/o software base en las computadoras, solo podrá realizarlo el personal autorizado por la OSNIRH. En ningún caso el trabajador intentará reparar la anomalía o falla, ni abrir los equipos de cómputo ni modificar la configuración de los equipos bajo las responsabilidades respectivas.



5.9.5 Del Mantenimiento de los Servidores Institucionales

- a. Los servidores centrales deben contar con un plan de mantenimiento preventivo y correctivo permanente, que asegure la provisión de repuestos necesarios y operatividad de los servidores centrales de forma inmediata. Este plan debe considerar tanto el hardware como contratos de mantenimiento y soporte para el software base.
- b. El Administrador de Red de la ANA, deberá realizar el afinamiento permanente del rendimiento de los servidores a nivel de procesamiento y capacidad en disco, para lo cual debe realizar un planeamiento anual de crecimiento y/o actualización de equipo de cómputo de acuerdo al crecimiento proyectado por la organización en su conjunto.



VI. MECÁNICA OPERATIVA

6.1 La OSNIRH entregará los equipos de cómputo al usuario con el software y hardware instalado, lo cual quedará oficializado en un acta de entrega de equipos de cómputo y software. Se verificará la información del acta después de hecho el inventario planeado dos (2) veces al año y se verificará la información de acuerdo al acta firmada.

6.2 Para realizar la copia de seguridad, se tendrá en cuenta:

- a. Backup Central: Se realizará una copia de respaldo de los documentos institucionales en un Servidor Central, para ello se le indicará al usuario en que carpeta de su PC deberá guardar los archivos a salvaguardar.



- b. Backup Personal: Cada usuario es responsable de realizar la copia de respaldo de su información a salvaguardar, esta deberá hacerse en medios magnéticos "USB, DVD" y será guardada por los usuarios.

6.3 La OSNIRH cuenta con una consola central de antivirus, la cual permite actualizar, detectar y eliminar virus en las PC. Se instalará un agente de antivirus en cada PC de la Institución para ser monitoreado desde el servidor central; además, es necesario que cada usuario programe de manera local el escaneo de virus en sus discos locales.

6.4 Para la implementación de sistemas de información.

- a. El área usuaria deberá describir la necesidad de producto o servicio de software, que puede determinar la adquisición, desarrollo o mantenimiento del mismo. Para la descripción de esta necesidad, deberá utilizar el Formato de Requerimiento de Software (Anexo 5).



- b. El área usuaria remitirá el Formato de Requerimiento de Software (Anexo 5) debidamente llenado, a la Oficina del Sistema Nacional de Información de Recursos Hídricos (OSNIRH), para su evaluación y posterior definición de los requerimientos.

- c. La OSNIRH encarga a un profesional (Analista de Sistemas) que estudie la necesidad, y posteriormente concierta una cita con el área usuaria para profundizar en los requerimientos. El área usuaria indicará quien/es es/son el/los usuario/s líder/es del sistema para poder ser entrevistado/s. Se creará un expediente físico y se registrará el documento de requerimiento de software.



- d. El profesional de la OSNIRH (Analista de Sistemas) se reunirá con el/los usuario/s líder/es del sistema, y por intermedio de técnicas de entrevista, encuesta y otras, identificará los requerimientos del sistema, lo registrará en el Formato de Requerimientos (Anexo 6), y se dejará registro de las reuniones a través del Formato Acta de Reunión (Anexo 7).

- e. Si culminada la cita y dada la conformidad, los profesionales del área usuaria y OSNIRH quedan claros en los requerimientos del sistema, se firmará por los participantes el acta de reunión y la matriz de requerimiento identificada. En caso contrario, se firmará solamente por los participantes el acta de reunión, se concertará una nueva cita para afinar los requerimientos y se deberá hacer referencia a la matriz de requerimiento como borrador de avance. Cualquiera sea el caso, el Analista de Sistemas registrará los documentos obtenidos.



- f. El Analista de Sistemas analizará los requerimientos del sistema hasta el momento obtenidos, proyectando el alcance, tiempo y costo, y cruzándolo con los recursos y presupuesto disponibles y criticidad para la organización; definirá las acciones a tomar (desarrollar, mantener o adquirir) para obtener el producto o servicio de software y el inicio del proyecto.



- g. Sea el caso que no es factible tomar acción en el presente periodo, se le comunicará al área usuaria dicho hecho en la brevedad posible y se archivará el expediente.

- h. Con la Matriz de requerimientos identificada, el Analista de Sistemas definirá y documentará los requerimientos del sistema, empleando diagramas (casos de uso) y plantillas (especificación de casos de uso) para dicho fin, los cuales deberán ser comprensibles por el área usuaria.



- i. El Analista de Sistema citará a los especialistas en las tecnologías de información, para exponerle los requerimientos definidos y posteriormente, en forma conjunta bosquejar una propuesta de solución técnica. La propuesta de solución se



documentará en el Formato de Definición del Proyecto (Anexo 8), donde se definirá el Alcance del Proyecto, Cronograma de actividades, Riesgos, Objetivos, Recursos, Entregables, Costos, acción a tomar (desarrollar, mantener o adquirir), y la descripción del proyecto en el cual se plantearán la Arquitectura del Sistema, Ámbito del Sistema y Prototipo de Interfaces.

- j. El Analista de Sistemas citará al área usuaria para presentarles la propuesta de solución con el documento de Definición de requerimientos. En dicha reunión, se expondrá la solución técnica encontrada y se esperará la aprobación del área usuaria. En dicha reunión, se dejará constancia de la reunión con el acta de reunión.
- k. En caso no se apruebe la propuesta de solución, se recogerán las observaciones, el Analista de Sistemas se reunirá con los especialistas en tecnologías de información y ajustarán la propuesta para nuevamente presentarla. En caso se apruebe, el Analista de Sistema informará del mismo al Director de la OSNIRH para que disponga su ejecución y anexará la propuesta de solución al expediente del proyecto.



6.5 Para el servicio de Soporte Técnico y Help Desk

- a. Se recibe la llamada telefónica de solicitud de servicio por parte del área de Help Desk.
- b. Se determina si la llamada amerita o no una atención por parte del área.
- c. Se registra la llamada en el sistema de atención como recibida y en curso.
- d. De acuerdo al tipo de incidente presentado, se designa a un especialista (hardware o software) para que se haga cargo del mismo.
- e. Se procede a la creación de la Ficha de Atención Técnica (Anexo 4) con los datos iniciales del usuario y el problema presentado.
- f. Se valida que el problema sea realmente el que reportó el usuario.
- g. Se evalúa la gravedad del problema y costo de tiempo/esfuerzo.
- h. En caso se determine que no puede solucionarse el problema en el mismo lugar del usuario, teniendo como tiempo máximo 45 minutos, debe dejársele un equipo de contingencia con el fin de no perjudicar la continuidad del trabajo del usuario.
- i. Se traslada el equipo al laboratorio para realizar tareas exhaustivas de revisión.
- j. En este punto se toman las acciones respectivas, dependiendo si el error es provocado por el software o el hardware del equipo.
- k. En caso de ser un problema de hardware, si el equipo se encuentra en garantía, se debe acudir al proveedor para seguir el procedimiento respectivo a la garantía.
- l. El Centro autorizado de servicio (CAS) autorizado por el proveedor recoge el equipo de la Autoridad Nacional del Agua para revisarlo en su laboratorio.
- m. Luego que el Centro autorizado de servicio (CAS) realice las acciones necesarias sobre el equipo (cambio total del equipo o de pieza), es devuelto a la Autoridad Nacional del Agua.
- n. En este punto, dependiendo del tipo de problema se realizan las acciones siguientes:



- Si el problema es de software: Se procede a realizar el respaldo de la configuración y datos del usuario, y se procede a reinstalar completamente el equipo en caso de ser necesario.
- Si el problema es de hardware: Se revisa el equipo en conjunto, si alguna de sus partes presenta alguna falla, trata de repararse; si esto no es posible, se realiza el cambio de la pieza afectada (con alguno de los repuestos en stock o se informa al área usuaria para que realice la compra de la misma).

ñ. Se indica si el problema pudo ser resuelto.

o. En el caso que el equipo o periférico no haya podido ser reparado, emite un informe al usuario para que proceda a efectuar los trámites para dar de baja al equipo.

p. Se determina si fue entregado temporalmente un equipo al usuario, para que pueda seguir laborando normalmente.

q. Se reemplaza el equipo de contingencia entregado temporalmente al usuario por su equipo original.

r. Se procede a completar la ficha técnica, para ello son indispensables las firmas del especialista y del usuario atendido.

s. Se ingresan los datos de la ficha técnica al sistema de atención al usuario.



VII. RESPONSABILIDAD

Los Directivos de los órganos de la sede central y los órganos desconcentrados de la Autoridad Nacional del Agua son responsables del cumplimiento de la presente Directiva General, en lo que les corresponda de acuerdo a su competencia.



VIII. ANEXOS

Forman parte de la presente Directiva los anexos siguientes:

Anexo 1: Acta de Entrega de Equipos de Cómputo (Hardware).

Anexo 2: Acta de Entrega de Software.

Anexo 3: Formato de Informe Técnico Previo de Evaluación de Software y/o Hardware.

Anexo 4: Formato de Ficha de Atención Técnica.

Anexo 5: Formato de Requerimiento de Software.

Anexo 6: Formato de Matriz de Requerimientos.

Anexo 7: Formato de Acta de Reunión.

Anexo 8: Formato de Definición del Proyecto.



CARLOS JAVIER PAGADOR MOYA

Jefe

Autoridad Nacional del Agua

Acta de Entrega de Hardware

Usuario: _____ Área: _____

A. N° de Serie CPU: _____ Dirección IP: _____

a. Tipo: _____
 Marca: _____ Modelo: _____ Tipo Case: _____

b. Tarjeta Madre: Marca: _____ Modelo: _____

c. Procesador: Marca: _____ Modelo: _____ Velocidad: _____ GHz.

d. Memoria RAM: Tipo: _____ Capacidad: _____ RAM Efectiva: _____

e. Tarjeta de Video: Tarjeta Integrada Tarjeta Externa
 Memoria de Video: _____ Marca: _____ Modelo: _____

f. Unidad de Disco Flexible: Si: No: Marca: _____ Capacidad: 1.44 MB

g. Disco Duro 0: Tipo: S-ATA
 Marca: _____ Modelo: _____ Capacidad: _____

h. Unidad Disco Duro Externo: Si: No:
 Marca: _____ Modelo: _____ Capacidad: _____

i. Unidad Óptica: Multi Grabador DVD/CD-RW Blu-Ray
 Marca: _____ Modelo: _____ Velocidad: _____

j. Lector de Memoria: Tipo: _____ Marca: _____ Modelo: _____

k. Tarjeta de Red: Tipo: _____ Marca: _____ Modelo: _____

B. Teclado: Marca: _____ Modelo: _____ Cod. Patrimonial: _____

C. Mouse: Tipo: _____ Marca: _____ Modelo: _____ Serie: _____

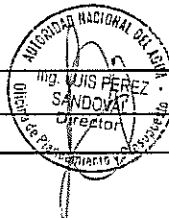
D. Parlantes: Tipo: _____ Marca: _____ Modelo: _____

E. Micrófono: Tipo: _____ Marca: _____ Modelo: _____

F. Cámara Web: Marca: _____ Modelo: _____ Serie: _____

G. Monitor: Marca: _____ Modelo: _____ Serie: _____
 Código Patrimonial: _____

Observaciones:



Firma del Usuario

Firma del Especialista



Acta de Entrega de Software

Usuario: _____ Área: _____

Sistema Operativo:
Windows Vista Ultimate de 64 Bit

Número de Serie: _____

Número de Licencia: _____

Software de Ofimática:

Microsoft Office:

Word Outlook Access Versión: 2003 2007 2010

Excel Powerpoint Frontpage Otros: Publisher 2003

Número de Licencia: _____

Open Office Versión: _____

Otros: _____ Número de Licencia: _____

Utilitarios:

Acrobat Reader Versión: 7.0 Número de Licencia: Freeware

Winzip Versión: _____ Número de Licencia: _____

Power DVD Versión: _____ Número de Licencia: _____

Nero Versión: StartSmart Número de Licencia: _____

Otros: _____

_____ Versión: _____ Número de Licencia: _____

_____ Versión: _____ Número de Licencia: _____

_____ Versión: _____ Número de Licencia: _____

_____ Versión: _____ Número de Licencia: _____

_____ Versión: _____ Número de Licencia: _____

Antivirus:

Observaciones: _____

Firma del Usuario



Firma del Especialista



PERÚ

Ministerio de
Agricultura

Autoridad Nacional
del Agua

Organismo del Sistema Nacional de
Información de los Recursos Hídricos

ANEXO 3

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE Y/O HARDWARE


N° __-2011-ANA-OSNIRH

1. Nombre del Área.
2. Responsable de la Evaluación
3. Cargos
4. Fecha
5. Justificación.
6. Alternativas.
7. Análisis Comparativo Técnico
8. Análisis Comparativo de Costo-Beneficio:
9. Conclusiones:
10. Firmas:

Profesional
Cargo
Autoridad Nacional del Agua



ANEXO 4

 <small>AUTORIDAD NACIONAL DEL AGUA</small>	Procedimiento 0004-2011-TI	Formato de Ficha de atención Técnica	Versión 1.0	<small>MINISTERIO DE AGRICULTURA</small> <small>AUTORIDAD NACIONAL DEL AGUA</small>
Pág. 1 de 1	Autoridad Nacional del Agua			

N° :
Fecha : / /

Usuario		
Dirección / Oficina / Unidad		Anexo:

<table border="1"> <thead> <tr> <th>Equipo</th> <th>Cod. Patrim.</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> CPU</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Monitor</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Teclado</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Impresora</td> <td></td> </tr> <tr> <td><input type="checkbox"/></td> <td></td> </tr> </tbody> </table>	Equipo	Cod. Patrim.	<input type="checkbox"/> CPU		<input type="checkbox"/> Monitor		<input type="checkbox"/> Teclado		<input type="checkbox"/> Impresora		<input type="checkbox"/>		Hora de Llamada : Hora Inicio : Hora Término : PROBLEMA: <div style="border: 1px solid black; height: 40px; width: 100%;"></div>
Equipo	Cod. Patrim.												
<input type="checkbox"/> CPU													
<input type="checkbox"/> Monitor													
<input type="checkbox"/> Teclado													
<input type="checkbox"/> Impresora													
<input type="checkbox"/>													

DIAGNOSTICO:

CATEGORÍA :	CLASE :
--------------------	----------------

TIPO DE LA ATENCION :

Reparación
 Mant. Preventivo
 Instalación Software y/o Hardware
 Configuración
 Capacitación

Otros:

ACCIÓN REALIZADA:

RECOMENDACIONES:

- RESULTADO DE LA ATENCION**
- Por Garantía y/o Cambio de Repuestos
 - Reparado
 - No Reparable
 - Operativo

- PENDIENTE:**
- Por Garantía
 - Por Repuestos (Por Informe)
 - Por Coordinación con el Usuario


Nombre del Técnico:.....



Firma del Técnico

Firma Usuario

ANEXO 5

 <small>AUTORIDAD NACIONAL DEL AGUA</small>	Procedimiento 0004-2011-TI	Formato de Requerimiento de Software	Versión 1.0	<small>MINISTERIO DE AGRICULTURA AUTORIDAD NACIONAL DEL AGUA</small>
Pág. 1 de 1	Autoridad Nacional del Agua			

Solicitante:..... Fecha: / /

Dirección/Unidad:..... Cargo:.....

Correo: Anexo:.....

Nombre de su Director:.....

Detalle de la Solicitud

¿Qué acción pretende?

Adquirir Desarrollar Dar Mantenimiento:

¿Qué es lo que desean Adquirir?

Sistema Software Módulo

Especificar nombre:

.....

¿Quiénes serán los beneficiarios?

¿Qué es lo que mejoraría? Procesos Actividades Tareas

¿Cómo lo mejoraría?.....

Mencionar que objetivos estratégicos cumpliría:

.....

Descripción de la solicitud:

.....


Tipo de Prioridad: Alta Media Baja

Solicitante

Director Inmediato

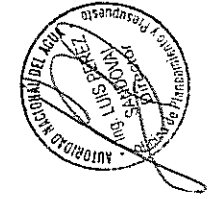
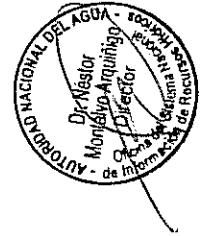


ANEXO 6


	Procedimiento 0005-2011-TI	Formato Matriz de Requerimientos	Versión 1.0	MINISTERIO DE AGRICULTURA AUTORIDAD NACIONAL DEL AGUA
Pág. 1 de 1		Autoridad Nacional del Agua		

MATRIZ DE REQUERIMIENTOS

Requerimientos		Tipo	Prioridad	Riesgo	Dependencia	Estado
ID	Titulo Descripción					
R1						
R2						
R3						
R4						
R5						



ANEXO 7

 <small>AUTORIDAD NACIONAL DEL AGUA</small>	Procedimiento 0006-2011-TI	Acta de Reunión N°	Versión 1.0	<small>MINISTERIO DE AGRICULTURA</small> <small>AUTORIDAD NACIONAL DEL AGUA</small>
Pág. 1 de 1	Autoridad Nacional del Agua			

Programación
 Datos sobre la reunión:

Ubicación:	
Fecha y Hora:	
Hora de Inicio:	
Hora de Fin:	

Objetivos
 A continuación los objetivos de la reunión:

<Describir los objetivos de la reunión>

Agenda
 Los temas de la agenda que se tratarán son:

<Describir la agenda de la reunión>

PARTICIPANTES
 Describir a los usuarios que asistieron a la reunión:

Usuarios			
Nombres	Cargo	Hora	
		Llegada	Salida

Proveedores			
Nombres	Cargo	Hora	
		Llegada	Salida



Temas tratados

<5.1 Tema tratado Nro. 1>

<5.2 Tema tratado Nro. 2>

Requerimientos pendientes (Si Los Hubiera, Según Agenda)

Por <indicar el motivo> se no se pudo tratar el siguiente requerimiento:

<Requerimiento 1>

<Requerimiento 2>

Acuerdos

<7.1 Acuerdo 1>

<7.2 Acuerdo 2>

LISTA DE DISTRIBUCIÓN

La presente acta se distribuirá a las personas siguientes personas:

<Persona 1>

<Persona 2>

Firmas

En señal de conformidad del contenido de la presente acta de reunión los asistentes proceden a firmarla en señal de conformidad.

V°B° Persona 1

V°B° Persona 2



ANEXO 8

	<p align="center">Definición del Proyecto</p>	<p align="center">MINISTERIO DE AGRICULTURA AUTORIDAD NACIONAL DEL AGUA</p>
<p>Pág. 1 de 7</p>	<p align="center"><Nombre del Proyecto></p>	

<Nombre del proyecto>

Código del Documento	Versión	Enfoque	Fecha de Vigencia	Total Páginas
OSNIRH_001_Definición del proyecto	1.0	General		08
Etapa	Nombre del Responsable	Firma	Fecha	
Revisado por:				
Aprobado por:				





Definición del Proyecto

MINISTERIO DE AGRICULTURA
AUTORIDAD NACIONAL DEL AGUA


Pág. 2 de 7

<Nombre del Proyecto>

TABLA DE CONTENIDOS

1.	Nombre del Proyecto.....	3
2.	Responsables del Proyecto.....	3
3.	Descripción del Proyecto.....	3
4.	Objetivos del Proyecto.....	3
5.	Alcance del Proyecto	3
5.1.	Marco Teórico	3
5.2.	Alcance.....	3
6.	Responsabilidades del Equipo de Trabajo	6
7.	Recursos.....	6
8.	Principales Entregables / Hitos.....	5
9.	Diagrama GANTT	6
10.	Riesgo Inicial del Proyecto.....	7
10.1.	Identificación de Riesgos	7
10.2.	Respuesta a Riesgo.....	7
11.	Presupuesto.....	8



	Definición del Proyecto	MINISTERIO DE AGRICULTURA AUTORIDAD NACIONAL DEL AGUA
Pág. 3 de 7	<Nombre del Proyecto>	

Nombre del Proyecto

1. Responsables del Proyecto

Responsable de Proyecto: (TI)	
Responsable de Proyecto: (Cliente Interno)	

Tabla 1

2. Descripción del Proyecto

3. Objetivos del Proyecto

4. Alcance del Proyecto

4.1. Marco Teórico

4.2. Alcance

5. Responsabilidades del Equipo de Trabajo

Responsabilidad	Nombre	Cargo

Tabla 2

