INAMHI
INSTITUTO NACIONAL DE METEOROLOGIA E HIDROLOGIA

RESOLUCIÓN No. DE-076-2014

EL DIRECTOR EJECUTIVO DEL INSTITUTO NACIONAL DE METEOROLOGIA E HIDROLOGIA

CONSIDERANDO:

Que el INAMHI es una Institución de derecho público, con personalidad jurídica, con sede en la ciudad de Quito, capital de la República del Ecuador y con jurisdicción en todo el territorio nacional. Es el Organismo rector, coordinador y normalizador de la política nacional en todo lo que se refiere a la Meteorología e Hidrología y tiene entre sus funciones mantener y operar la red básica de estaciones Hidrometeorológicas del Ecuador, conforme lo establece el Decreto Supremo No. 3438, publicado en el Registro Oficial No. 839 del 25 de mayo de 1979.

Que el INAMHI, se encuentra adscrito a la Secretaria de Gestión de Riesgos, en virtud del Decreto Ejecutivo No. 391, publicado en el Segundo Suplemento del Registro Oficial No. 224 del 29 de junio de 2010.

Que la Constitución de la República, en su Art. 227, determina que la Administración Pública constituye un servicio a la colectividad que se rige por principios de eficacia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación.

Que mediante Acuerdos Ministeriales No. 804 y 837 de 29 de julio y 19 de agosto de 2011, respectivamente; la Secretaría Nacional de la Administración Pública creó la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación conformada por delegados del Ministerio de Telecomunicaciones y de la Sociedad de Información, la Secretaría Nacional de Inteligencia y la Secretaría Nacional de la Administración Pública y dentro de sus atribuciones tiene la de establecer lineamientos de seguridad informática, protección de infraestructura computacional y todo lo relacionado von ésta, incluyendo la información contenida para las entidades de la Administración Pública Central e Institucional.

Que la Administración Pública de forma integral y coordinada debe propender a minimizar o anular riesgos en la información así como proteger la infraestructura gubernamental, más aún si es estratégica, de los denominados ataques informáticos o cibernéticos.

Que la Comisión para la Seguridad Informática y de las tecnologías de la Información y Comunicación en referencia ha desarrollado el Esquema Gubernamental de Seguridad de la Información (EGSI), elaborada en base a la norma NTEINEN-ISO/IEC 27002 "Código de Práctica para la Gestión de la Seguridad de la Información".

Que el Art. 15, letra i) del Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva establece como atribución del Secretario Nacional de la Administración Pública impulsar los proyectos de estandarización en procesos, calidad y tecnologías de la información y comunicación.

Que el Secretario Nacional de la Administración Pública, expide el Acuerdo No. 166, mediante el cual dispone a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información, publicada en el Segundo Suplemento del Registro Oficial No. 88 de 25 de septiembre de 2013.

Que el Art. 2 del Acuerdo 166, determina que las entidades de la Administración Pública implementarán en un plazo de 18 meses el Esquema de Seguridad de la Información (EGSI).

Que la implementación del GSI realizará en cada institución de acuerdo al ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de Seguridad de la Información.

Que el Art. 3 del Acuerdo 166, manifiesta que las entidades designarán al interior de su entidad, un Comité de Seguridad de la Información, liderado con un Oficial de Seguridad de la Información, conforme lo establece el EGSI, cuya denominación deberá ser comunicada a la Secretaría Nacional de la Administración Pública, en el transcurso de 30 días posteriores a la emisión del presente Acuerdo.

Que el seguimiento y control a la implementación de la EGSI se realizará mediante el Sistema de Gestión por Resultados (GPR) u otras herramientas que para el efecto implemente la Secretaría de la Administración Pública.

Que la máxima autoridad de cada entidad es responsable de mantener la documentación de la implementación del EGSI debidamente organizada y registrada de acuerdo al procedimiento específico que para estos efectos establezca la Secretaría Nacional de la Administración Pública.

Que de conformidad a la Disposición Transitoria Primera del Acuerdo 166, la Secretaría Nacional de la Administración Pública, para efectivizar el control y seguimiento del EGSI institucional, en un plazo de 15 días creará un proyecto en el sistema GPR en el que se homogenice los hitos que deben cumplir las instituciones para implementar el EGSI.

Que mediante memorando No. INAMHI-DE-2014-0062-DE de 17 de enero de 2014, solicita a la Dirección de Asesoría Jurídica, la elaboración de la Resolución para la implementación del Esquema Gubernamental de Seguridad de le Información EGSI, integrada por la normativa general, normativa de uso de correo electrónico, acuerdo para uso aceptable de Internet y normativas para uso de Software y Hardware institucional,

En uso de las facultades legales y reglamentarias,

RESUELVE:

DICTAR LAS NORMATIVAS GENERALES PARA EL USO Y CONTROL DEL SISTEMA INTEGRAL INFORMÁTICO EN EL INSTITUTO NACIONAL DE METEOROLOGÍA E HIDROLOGÍA

POLÍTICAS DE SEGURIDAD INFORMÁTICA

ART. 1. OBJETIVO DE SEGURIDAD:

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a la Institución para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información. Estos riesgos que se enfrentan han llevado a que se desarrolle un documento de directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones del Instituto Nacional de Meteorología e Hidrología

En este sentido, las políticas de seguridad informática definidas partiendo desde el análisis de los riesgos a los que se encuentra propenso el INAMHI, surgen como una herramienta organizacional para concienciar a los funcionarios de la Institución sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la Institución crecer y mantenerse competitiva.

Ante esta situación, el proponer nuestra política de seguridad requiere un alto compromiso con la Institución, agudeza técnica para establecer fallas y debilidades en su aplicación, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea al INAMHI.

ART.2. ALCANCE:

Este manual de políticas de seguridad se ha elaborado de acuerdo a los riesgos y vulnerabilidades que se han dado en distintos lugares de similar característica que el Instituto Nacional de Meteorología e Hidrología por consiguiente el alcance de estas políticas, se encuentra sujeto a la Institución.

ART. 3. OBJETIVOS GENERALES Y ESPECÍFICOS:

Desarrollar un sistema de seguridad, significa "planear, organizar, dirigir y controlar las actividades para mantener y garantizar la integridad física de los recursos informáticos, así como resguardar los activos de la Institución".

Los objetivos específicos, que se desean alcanzar luego de implantar nuestro sistema de seguridad, son los siguientes:

- Establecer un esquema de seguridad con perfecta claridad y transparencia bajo la responsabilidad del INAMHI en la administración del riesgo.
- Compromiso de todo el personal de la Institución con el proceso de seguridad, agilizando la aplicación de los controles con dinamismo y armonía.
- Que la prestación del servicio de seguridad gane en calidad, eficiencia y eficacia.
- Todos los empleados se convierten en interventores del sistema de seguridad.

ART. 4. RESPONSABILIDADES:

Es responsabilidad del Administrador de Aplicaciones, desarrollar, someter a revisión y divulgar en adición a los demás medios de difusión (intranet, email, sitio web oficial, revistas internas) de los Procedimientos de Seguridad. Asimismo, es responsabilidad del responsable del área de TIC's capacitar a sus empleados en lo relacionado con los Procedimientos de Seguridad.

ART. 5. DEFINICIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA:

Las políticas de seguridad, son un recurso para mitigar los riesgos a los que el Instituto Nacional de Meteorología e Hidrología se ve expuesto.

a. POLÍTICAS GENERALES:

1. La presente normativa, tiene por objeto estandarizar y contribuir al desarrollo informático de las diferentes áreas del INAMHI.

2. Para los efectos de este instrumento se entenderá por:

Comité:

Al equipo integrado por el área de TIC's, los Jefes de área y el personal administrativo (ocasionalmente) convocado para fines específicos como:

- Adquisiciones de hardware y software
- Establecimiento de estándares del INAMHI tanto de hardware como de software.
- Establecimiento de la Arquitectura tecnológica de grupo.
- Establecimiento de lineamientos para concursos de ofertas

Administración de informática:

Está integrada por el área de TIC's y Jefes de área, las cuales son responsables de:

- Velar por el funcionamiento de la tecnología informática que se utilice en las diferentes áreas.
- Definir estrategias y objetivos a corto, mediano y largo plazo
- Mantener la Arquitectura tecnológica
- Controlar la calidad del servicio brindado
- Mantener el Inventario actualizado de los recursos informáticos
- Velar por el cumplimiento de las Políticas y Procedimientos establecidos.

Políticas de Informática:

- Para los efectos de esta normativa, se entiende por Políticas en Informática, al conjunto de reglas obligatorias, que deben observar los Funcionarios de TIC's responsables del hardware y software existentes en el INAMHI, siendo responsabilidad de la Administración de Informática, vigilar su estricta observancia en el ámbito de su competencia, tomando las medidas preventivas y correctivas para que se cumplan.
- Las Políticas en Informática, son el conjunto de ordenamientos y lineamientos enmarcados en el ámbito jurídico y administrativo del INAMHI. Estas normas inciden en la adquisición y el uso de los Bienes y Servicios Informáticos, las cuales se deberán de acatar invariablemente, por aquellas instancias que intervengan directa y/o indirectamente en ello.
- La instancia rectora de los sistemas de informática del INAMHI es el Área de TIC's, y el organismo competente para la aplicación de este ordenamiento, es el Comité.
- Las Políticas aquí contenidas, son de observancia para la adquisición y uso de bienes y servicios informáticos en el INAMHI, cuyo incumplimiento generará que se incurra en responsabilidad administrativa; sujetándose a lo dispuesto en el reglamento interno de personal.

Lineamientos para la adquisición de bienes informáticos

- Toda adquisición de tecnología informática, se efectuará a través del Comité, que está conformado por el personal del área de TIC's conjuntamente con los peticionarios de la adquisición.
- La adquisición de bienes de Informática en el INAMHI, quedará sujeta a los lineamientos establecidos en este documento.

- La Administración de Informática, al planear las operaciones relativas a la adquisición de Bienes informáticos, establecerá prioridades y en su selección deberá tomar en cuenta: estudio técnico, precio, calidad, experiencia, desarrollo tecnológico, estándares y capacidad, entendiéndose por:

Precio.- Costo inicial, costo de mantenimiento y consumibles por el período estimado de uso de los equipos;

Calidad.- Parámetro cualitativo que especifica las características técnicas de los recursos informáticos.

Experiencia.- Presencia en el mercado nacional e internacional, estructura de servicio, la confiabilidad de los bienes y certificados de calidad con los que se cuente.

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

Estándares.- Toda adquisición se basa en los estándares, es decir la arquitectura de grupo Institución establecida por el Comité. Esta arquitectura tiene una permanencia mínima de dos a cinco años.

Capacidades.- Se deberá analizar si satisface la demanda actual con un margen de holgura y capacidad de crecimiento para soportar la carga de trabajo del área.

Para la adquisición de Hardware:

- El equipo que se desee adquirir deberá estar dentro de las listas de ventas vigentes de los fabricantes y/o distribuidores del mismo.
- Los equipos complementarios deberán tener una garantía mínima de un año y deberán contar con el servicio técnico correspondiente en el país.
- Deberán ser equipos integrados de fábrica o ensamblados con componentes previamente evaluados por el Comité.
- La marca de los equipos o componentes deberá contar con presencia y permanencia demostrada en el mercado nacional e internacional, así como con asistencia técnica y refaccionaria local. Tratándose de microcomputadores, a fin de mantener actualizada la arquitectura informática del INAMHI.
- Los dispositivos de almacenamiento, así como las interfaces de entrada / salida, deberán estar acordes con la tecnología de punta vigente, tanto en velocidad de transferencia de datos, como en procesamiento.
- Las impresoras deberán sejetarse a los estándares de Hardware y Software vigentes en el mercado y en el INAMHI, corroborando que los suministros (tóner, cintas, papel, etc.) se consigan fácilmente en el mercado y no estén sujetas a un solo proveedor.
- Conjuntamente con los equipos, se deberá adquirir el equipo complementario adecuado para su correcto funcionamiento de acuerdo con las especificaciones de los fabricantes, y que esta adquisición se manifieste en el costo de la partida presupuestaria.
- Los equipos adquiridos deben contar, de preferencia con asistencia técnica durante la instalación de los mismos.
- En lo que se refiere a los servidores, equipos de comunicaciones, concentradores de medios (HUBS) y otros equipos que se justifiquen por ser de operación crítica y/o de alto costo, deben de contar con un programa de mantenimiento preventivo y correctivo que incluya el suministro de refacciones al vencer su período de garantía.
- En lo que se refiere a los computadores denominados personales, al vencer su garantía por adquisición, deben de contar por lo menos con un programa de servicio de mantenimiento correctivo que incluya el suministro de refacciones.
-
- Todo proyecto de adquisición de bienes de informática, debe sujetarse al análisis, aprobación y autorización del Comité.
- En la adquisición de Equipo de cómputo se deberá incluir el Software vigente precargado con su licencia correspondiente considerando las disposiciones del artículo siguiente.

Para la adquisición de Software:

- Base y utilitarios, el Comité dará a conocer periódicamente las tendencias con tecnología de punta vigente, siendo la lista de productos autorizados la siguiente:

Plataformas de Sistemas Operativos
- Windows
- Linux

Bases de Datos
- Postgres
- Oracle

Lenguajes y herramientas de programación
- PHP
- Flex
- Java

Utilitarios de oficina
- Microsoft Office
- Koffice

Programas antivirus
- Kaspersky

Manejador de correo electrónico
- Outlook
- Thunderbird

Navegadores de Internet
- Internet Explorer
- Mozilla

Comprimidores de archivos
- Winzip
- Winrar

En casos excepcionales, sólo se adquirirán las últimas versiones liberadas de los productos seleccionados, salvo situaciones específicas que se deberán

justificar ante el Comité. Todos los productos de Software que se adquieran deberán contar con su licencia de uso, documentación y garantías respectivas.

- Todos los productos de Software que se utilicen a partir de la fecha en que entre en vigor el presente documento, deberán contar con su licencia de uso respectiva; por lo que se promoverá la regularización o eliminación de los productos ya instalados que no cuenten con el debido licenciamiento.
- Para la operación del software de red en caso de manejar los datos Institucionales mediante sistemas de información, se deberá tener en consideración lo siguiente:
- Toda la información institucional deberá invariablemente ser operada a través de un mismo tipo de sistema manejador de base de datos para beneficiarse de los mecanismos de integridad, seguridad y recuperación de información en caso de presentarse alguna falla.
- El acceso a los sistemas de información, deberá contar con los privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad total de la información institucional. Los niveles de seguridad de acceso deberán controlarse por un administrador único y poder ser manipulado por software.
- Se deben delimitar las responsabilidades en cuanto a quién está autorizado a consultar y/o modificar en cada caso la información, tomando las medidas de seguridad pertinentes.
- Los datos de los sistemas de información, deben ser respaldados de acuerdo a la frecuencia de actualización de sus datos, rotando los dispositivos de respaldo y guardando respaldos históricos periódicamente. Es indispensable llevar una bitácora oficial de los respaldos realizados, asimismo, los CDs de respaldo deberán guardarse en un lugar de acceso restringido con condiciones ambientales suficientes para garantizar su conservación. En cuanto a la información de los equipos de cómputo personales, el área de TIC's recomienda a los usuarios que realicen sus propios respaldos en la red o en medios de almacenamiento alternos.
- Todos los sistemas de información que se tengan en operación, deben contar con sus respectivos manuales actualizados. Un técnico que describa la estructura interna del sistema así como los programas, catálogos y archivos que lo conforman y otro que describa a los usuarios del sistema y los procedimientos para su utilización.
- Los sistemas de información, deben contemplar el registro histórico de las transacciones sobre datos relevantes, así como la clave del usuario y fecha en que se realizó (Normas Básicas de Auditoria y Control).
- Se deben implantar rutinas periódicas de auditoria a la integridad de los datos y de los programas de cómputo, para garantizar su confiabilidad.
- Para la prestación del servicio de desarrollo o construcción de Software aplicativo se observará lo siguiente:
- Todo proyecto de contratación de desarrollo o construcción de software requiere de un estudio de factibilidad que permita establecer la rentabilidad del proyecto así como los beneficios que se obtendrán del mismo.

ART.6. INSTALACIONES DE LOS EQUIPOS DE CÓMPUTO:

La instalación del equipo de cómputo, quedará sujeta a los siguientes lineamientos:

- Los equipos para uso interno se instalarán en lugares adecuados, lejos de polvo y tráfico de personas.
- El área de TIC's así como las áreas operativas deberán contar con un croquis actualizado de las instalaciones eléctricas y de comunicaciones del equipo de cómputo en red.
- Las instalaciones eléctricas y de comunicaciones, estarán de preferencia fija o en su defecto resguardadas del paso de personas o máquinas, y libres de cualquier interferencia eléctrica o magnética.
- Las instalaciones se apegarán estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios.
- En ningún caso se permitirán instalaciones improvisadas o sobrecargadas.
- La supervisión y control de las instalaciones se llevará a cabo en los plazos y mediante los mecanismos que establezca el Comité.

ART. 7. LINEAMIENTOS EN INFORMÁTICA:

a. INFORMACIÓN:

- La información almacenada en medios magnéticos se deberá inventariar, anexando la descripción y las especificaciones de la misma, clasificándola en tres categorías:
- Información histórica para auditorias.
- Información de interés de la Institución
- Información de interés exclusivo de alguna área en particular.
- Los jefes de área responsables de la información contenida en los departamentos a su cargo, delimitarán las responsabilidades de sus subordinados y determinarán quien está autorizado a efectuar operaciones emergentes con dicha información tomando las medidas de seguridad pertinentes.
- Se establecen tres tipos de prioridad para la información:
- Información vital para el funcionamiento del área;
- Información necesaria, pero no indispensable en el área.
- Información ocasional o eventual.
- En caso de información vital para el funcionamiento del área, se deberán tener procesos colaborativos, así como tener el respaldo diario de las modificaciones efectuadas, rotando los dispositivos de respaldo y guardando respaldos históricos semanalmente.
- La información necesaria pero no indispensable, deberá ser respaldada con una frecuencia mínima de una semana, rotando los dispositivos de respaldo y guardando respaldos históricos mensualmente.
- El respaldo de la información ocasional o eventual queda a criterio del área.
- La información almacenada en medios magnéticos, de carácter histórico, quedará documentada como activos del área y estará debidamente resguardada en su lugar de almacenamiento.
- Es obligación del responsable del área, la entrega conveniente de la información, a quien le suceda en el cargo.
- Los sistemas de información en operación, como los que se desarrollen deberán contar con sus respectivos manuales. Un manual del usuario que describa los procedimientos de operación y el manual técnico que describa su estructura interna, programas, catálogos y archivos.
- Ningún colaborador en proyectos de software y/o trabajos específicos, deberá poseer, para usos no propios de su responsabilidad, ningún material o información confidencial del INAMHI tanto ahora como en el futuro.

ART. 8. FUNCIONAMIENTO DE LOS EQUIPOS DE CÓMPUTO:

Es obligación del Administrador de aplicaciones vigilar que el equipo de cómputo se use bajo las condiciones especificadas por el proveedor y de acuerdo a las funciones del área a la que se asigne.

Los funcionarios de la Institución al usar el equipo de cómputo, se abstendrán de consumir alimentos, fumar o realizar actos que perjudiquen el funcionamiento del mismo o deterioren la información almacenada en medios magnéticos, ópticos, o medios de almacenamiento removibles de última generación.

Por seguridad de los recursos informáticos se deben establecer las siguientes seguridades:

- Físicas
- Sistema Operativo
- Software
- Comunicaciones
- Base de Datos
- Proceso
- Aplicaciones

Por ello se establecen los siguientes lineamientos:

- Mantener claves de acceso que permitan el uso solamente al personal autorizado para ello.
- Verificar la información que provenga de fuentes externas a fin de corroborar que esté libre de cualquier agente contaminante o perjudicial para el funcionamiento de los equipos.
- Mantener pólizas de seguros de los recursos informáticos en funcionamiento

En ningún caso se autorizará la utilización de dispositivos ajenos a los procesos informáticos del área. Por consiguiente, se prohíbe el ingreso y/o instalación de hardware y software particular, es decir que no sea propiedad del INAMHI, excepto en casos emergentes que el área de TIC's autorice.

Para la elaboración de los proyectos informáticos y para la determinación presupuestaria de los mismos, se tomarán en cuentan tanto las necesidades de hardware y software del área solicitante, como la disponibilidad de recursos con los que cuente el INAMHI.

Art. 9. ACCESO FÍSICO:

Únicamente al personal autorizado le está permitido el acceso a las instalaciones donde se almacena la información confidencial del INAMHI.

Sólo bajo la vigilancia de personal autorizado, puede el personal externo entrar en las instalaciones donde se almacena la información confidencial, y durante un periodo de tiempo justificado.

ART. 10. IDENTIFICADORES DE USUARIO Y CONTRASEÑAS:

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

Ningún usuario recibirá un identificador de acceso a la Red de Comunicaciones, Recursos Informáticos o Aplicaciones hasta que no acepte formalmente la Política de Seguridad vigente.

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

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

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

ART. 10. RESPONSABILIDADES PERSONALES:

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

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

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

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

El Usuario debe utilizar una contraseña compuesta por un mínimo de ocho caracteres constituida por una combinación de caracteres alfabéticos, numéricos y especiales.

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

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

En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada 30 días. En caso contrario, se le podrá denegar el acceso y se deberá contactar con el jefe inmediato para solicitar al administrador de la red una nueva clave.

Proteger, en la medida de sus posibilidades, los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o accidentales.

modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentren contenidos los datos.

Guardar por tiempo indefinido la máxima reserva y no se debe emitir al exterior datos de carácter personal contenidos en cualquier tipo de soporte.

Utilizar el menor número de listados que contengan datos de carácter personal y mantener los mismos en lugar seguro y fuera del alcance de terceros.

Cuando entre en posesión de datos de carácter personal, se entiende que dicha posesión es estrictamente temporal, y debe devolver los soportes que contienen los datos inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos.

Los usuarios sólo podrán crear ficheros que contengan datos de carácter personal para un uso temporal y siempre necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán ubicados en unidades locales de disco de la computadora de trabajo y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.

Los usuarios deben notificar a su jefe inmediato cualquier incidencia que detecten que afecte o pueda afectar a la seguridad de los datos de carácter personal: pérdida de listados y/o usbs, sospechas de uso indebido del acceso autorizado por otras personas, recuperación de datos.

Los usuarios únicamente introducirán datos identificativos y direcciones o teléfonos de personas en las agendas de contactos de las herramientas ofimáticas (por ejemplo en Thunderbird)

ART. 11.SALIDA DE INFORMACIÓN:

Toda salida de información (en soportes informáticos o por correo electrónico) sólo podrá ser realizada por personal autorizado y será necesaria la autorización formal del responsable del área del que proviene.

Además, en la salida de datos especialmente protegidos, se deberán cifrar los mismos o utilizar cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada durante su transporte.

ART. 12. USO APROPIADO DE LOS RECURSOS INFORMÁTICOS:

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

ART. 13. PROHIBICIONES:

El uso de estos recursos para actividades no relacionadas con el propósito de la institución, o bien con la extralimitación en su uso.

Las actividades, equipos o aplicaciones que no estén directamente especificados como parte del Software o de los Estándares de los Recursos Informáticos propios del INAMHI.

Introducir en los Sistemas de Información o la Red Institucional contenidos obscenos, amenazadores, inmorales u ofensivos.

Introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los Recursos Informáticos. El personal contratado por el INAMHI tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en los Sistemas de cualquier elemento destinado a destruir o corromper los datos informáticos.

Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.

Albergar datos de carácter personal en las unidades locales de disco de los computadores de trabajo.

Cualquier fichero introducido en la red institucional o en el puesto de trabajo del usuario a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual y control de virus.

ART. 14. USO DE SOFTWARE:

Todo el personal que accede a los Sistemas de Información del INMAHI, debe utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de utilización.

Todo el personal tiene prohibido instalar copias ilegales de cualquier programa, incluidos los estandarizados.

También tiene prohibido borrar cualquiera de los programas instalados legalmente.

ART. 15. RECURSOS DE RED:

De forma rigurosa, ninguna persona debe:

- Conectar a ninguno de los Recursos, ningún tipo de equipo de comunicaciones (Ej. módem) que posibilite la conexión a la Red Institucional.
- Conectarse a la Red Institucional a través de otros medios que no sean los definidos.
- Intentar obtener otros derechos o accesos distintos a aquellos que les hayan sido asignados.
- Intentar acceder a áreas restringidas de los Sistemas de Información o de la Red Institucional.
- Intentar distorsionar o falsear los registros "log" de los Sistemas de Información.
- Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos.
- Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros Usuarios, ni dañar o alterar los Recursos Informáticos.

ART.- 16. CONECTIVIDAD A INTERNET:

La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Todos los funcionarios del INAMHI tienen las mismas responsabilidades en cuanto al uso de Internet.

El acceso a Internet se restringe exclusivamente a través de la Red establecida para ello, es decir, por medio del sistema de seguridad con cortafuegos incorporado en la misma. No está permitido acceder a Internet llamando directamente a un proveedor de servicio de acceso y usando un navegador, o con otras herramientas de Internet conectándose con un módem.

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

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

En caso de tener que producirse una transmisión de datos importante, confidencial o relevante, sólo se podrán transmitir en forma encriptada.

ART.- 17. ACTUALIZACIONES DE LA POLÍTICA DE SEGURIDAD INFORMÁTICA:

Debido a la propia evolución de la tecnología y las amenazas de seguridad, y a las nuevas aportaciones legales en la materia, el INAMHI se reserva el derecho a modificar esta Política cuando sea necesario. Los cambios realizados en esta Política serán divulgados a todos los funcionarios del INAMHI.

ART. 18. BENEFICIOS DE IMPLANTAR POLÍTICAS DE SEGURIDAD INFORMÁTICA EN EL INAMHI:

Los beneficios de un sistema de seguridad con políticas claramente concebidas bien elaboradas son inmediatos, ya que el INAMHI trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos:

- Aumento de la productividad.
- Aumento de la motivación del personal.
- Compromiso con la misión de la Institución.
- Mejora de las relaciones laborales.
- Ayuda a formar equipos competentes.
- Mejora de los climas laborales para los Recursos Humanos.

POLÍTICAS INSTITUCIONALES

ART. 1. OBJETIVO:

El Instituto Nacional de Meteorología e Hidrología, reconoce los principios de libertad de expresión y privacidad de información como partes implicadas en el servicio de correo electrónico.

El INAMHI anima al uso del correo electrónico y respeta la privacidad de los usuarios.

No se procederá en forma rutinaria a realizar monitorizaciones o inspecciones de los buzones sin el consentimiento del propietario del buzón. Sin embargo podrá denegarse el acceso a los servicios de correo electrónico locales e inspeccionar, monitorizar y cancelar una cuenta de correo:

- Cuando haya requerimientos legales.
- Cuando haya sospechas fundadas de violación de la política interna de la institución, como comercio electrónico, falsificación de direcciones etc. Evitando caer en rumores, chismorreos u otras evidencias no fundadas y previo consentimiento del máximo responsable del servicio.
- Cuando por circunstancias de emergencia, donde no actuar pudiera repercutir gravemente en el servicio general a la comunidad.

ART. 2 POLÍTICAS GENERALES:

1. Nuestra institución es responsable de cualquier nombre de dominio DNS de tercer nivel bajo el dominio "inamhi.gob.ec".
2. Dentro de los servicios de comunicaciones que nuestra institución provee, se ofrecen cuentas de correo electrónico y una o varias máquinas para el encaminamiento y recogida de correo a/desde Internet a los buzones de las cuentas. Teniendo registro de las personas que los están utilizando bajo las direcciones electrónicas de las que somos responsables.
3. Como gestores del servicio de correo electrónico dentro de nuestra institución, nos reservamos el derecho de tomar las medidas sancionadoras oportunas contra los usuarios internos y externos que realicen cualquiera de los abusos determinados en la normativa.
4. Disponemos de suficiente información acerca de:

    - Las diversas actividades que trascienden los objetivos habituales del uso del servicio de correo electrónico que presta nuestra Institución.
    - Los perjuicios directos o indirectos que este problema ocasiona a nuestros propios usuarios, rendimientos de máquinas, líneas de comunicaciones etc.

ART. 3 DERECHOS:

1. Proteger la reputación y buen nombre de nuestra institución en la Red (Internet)
2. Garantizar la seguridad, rendimientos y privacidad de los sistemas de nuestra organización y de los demás.
3. Evitar situaciones que puedan causar a nuestra organización algún tipo de responsabilidad civil o penal.
4. Preservar la privacidad y seguridad de nuestros usuarios.
5. Proteger la labor realizada por las personas que trabajan en nuestros servicios de comunicaciones frente a ciertos actos indeseables

ART. 4. EFECTOS DE APLICACIÓN:

1. Todas las máquinas de nuestra Institución.
2. Todas las piezas de mensajes (texto, cabeceras y trazas) residentes en ordenadores propiedad de nuestra institución.
3. Todos los usuarios responsables de cuentas de correo en o bajo el dominio inamhi.gob.ec.

Esta política sólo se aplica al correo electrónico en formato electrónico y no es aplicable a correo electrónico en formato papel.

ART. 5. COMPROMISOS INSTITUCIONALES:

1. Emplear los recursos técnicos y humanos a nuestro alcance para intentar evitar cualquiera de los tipos de abusos reflejados en este documento.
2. Proporcionar a los usuarios del servicio de correo electrónico del INAMHI los mecanismos necesarios para denunciar cualquier abuso que pudieran sufrir.
3. Intentar mantener nuestro servidor de correo institucional con las últimas mejoras técnicas (actualizaciones, parches, filtros etc.) para defenderlos de los ataques definidos en este documento.
4. Proteger los datos personales de nuestros usuarios: Nombre Apellidos y dirección de correo electrónico de acuerdo con la Ley.
5. Intentar impedir y perseguir a usuarios internos que realicen cualquiera de las actividades definidas en la presente normativa.
6. Dedicar un buzón (abuse@inamhi.gov.ec) donde puedan ser enviados y atendidos los incidentes originados desde nuestra organización, así como las consultas y quejas de nuestros usuarios

ART. 6. ABUSO EN EL CORREO ELECTRÓNICO (ACE):

Se define ACE (Abuso en Correo Electrónico) como las diversas actividades que trascienden los objetivos habituales del servicio de correo y perjudican directa o indirectamente a los usuarios.

Algunos de los términos en inglés habitualmente asociados en Internet a estos tipos de abuso son *spamming*, *mail bombing (bombardeo de correo)*, *unsolicited bulk email* (UBE), *unsolicited commercial email* (UCE), *junk mail*, etc., abarcando un amplio abanico de formas de difusión. Los términos transformados a castellano son: correo basura, correo no solicitado, etc.

De los tipos de abuso englobados en ACE, el que más destaca es el conocido como *spam* que es un término aplicado a mensajes distribuidos a una gran cantidad de destinatarios de forma indiscriminada. En la mayoría de los casos el emisor de estos mensajes es desconocido y generalmente es imposible responderlo (*reply*) de la forma habitual o incluso llegar a identificar una dirección de retorno correcta.

ART. 7. DEFINICIÓN DE TÉRMINOS TÉCNICOS:

El correo en Internet es procesado por máquinas o servidores de origen, de encaminamiento y de destino utilizando el estándar de correo SMTP. Los agentes implicados en la transferencia de correo son:

- ***Operador de Origen***: Es la organización responsable de la máquina que encamina el mensaje de correo hacia Internet.
- ***Operador de Encaminamiento***: Es la organización responsable de las máquinas que encaminan el mensaje de correo entre el operador de origen y el operador de destino).
- ***Operador de Destino***: Es la organización o responsable de la máquina que mantiene el control de los buzones de los destinatarios.
- ***Emisor***: Es la persona origen del mensaje. Incluso cuando el emisor es un programa o sistema operativo, habrá una o más personas que sea(n) responsable(s) del mismo.
- ***Receptor***: Es la persona que recibe el mensaje. Al igual que en el caso del receptor, puede no tratarse de una persona física, pero siempre habrá al menos un responsable más o menos directo de cada dirección de destino.
- ***Listas de correo***: Son receptores de correo que actúan distribuyendo el mensaje a un número de destinatarios. Se las puede considerar como una especie de en caminadoras de correo. Estas listas pueden ser gestionadas por una persona o por un proceso automático

No se les considera emisores, ni receptores propiamente dichos, ya que la lista no es ni el origen ni el destinatario final de los mensajes. Sin embargo, pueden considerarse como tal en algunos casos: por ejemplo, los mensajes de control enviados para darse de alta o baja de una lista, y las respuestas del servidor a dichas acciones. Incluso en esos casos hay una persona detrás del servidor: el administrador del mismo

ART. 8. TIPOS DE ABUSO DE APLICACIÓN:

Las actividades catalogadas como ACE se pueden clasificar en cuatro grandes grupos:

a. Difusión de contenido inadecuado

Contenido ilegal por naturaleza (todo el que constituya complicidad con hechos delictivos). Ejemplos: apología del terrorismo, programas piratas, pornografía infantil, amenazas, estafas, esquemas de enriquecimiento piramidal, virus o código hostil en general.

Contenido fuera de contexto en un foro temático. Pueden definir lo que es admisible: el moderador del foro, si existe; su administrador o propietario, en caso contrario, o los usuarios del mismo en condiciones definidas previamente al establecerlo (por ejemplo, mayoría simple en una lista de correo).

b. Difusión a través de canales no autorizados

Uso no autorizado de una estafeta ajena para reenviar correo propio. Aunque el mensaje en sí sea legítimo, se están utilizando recursos ajenos sin su consentimiento (nada que objetar cuando se trata de una estafeta de uso público, declarada como tal.)

c. Difusión masiva no autorizada

El uso de estafetas propias o ajenas para enviar de forma masiva publicidad o cualquier otro tipo de correo no solicitado se considera inadecuado por varios motivos, pero principalmente éste: el anunciante descarga en transmisores y destinatarios el coste de sus operaciones publicitarias, tanto si quieren como si no quieren.

d. Ataques con objeto de imposibilitar o dificultar el servicio

Dirigido a un usuario o al propio sistema de correo. En ambos casos el ataque consiste en el envío de un número alto de mensajes por segundo, o cualquier variante, que tenga el objetivo neto de paralizar el servicio por saturación de las líneas, de la capacidad de CPU del servidor, o del espacio en disco de servidor o usuario. Se puede considerar como una inversión del concepto de difusión masiva (1->n), en el sentido de que es un ataque (n->1).

En inglés estos ataques se conocen como mail bombing, y son un caso particular de *denial of service* (DoS). En castellano podemos llamarlos bomba de correo o saturación, siendo un caso particular de denegación de servicio. Suscripción indiscriminada a listas de correo. Es una versión del ataque anterior, en la que de forma automatizada se suscribe a la víctima a miles de listas de correo. Dado que en este caso los ataques no vienen de una sola dirección, sino varias, son mucho más difíciles de atajar.

ART. 10. PROBLEMAS OCASIONADOS:

1. **Efectos en los receptores**

Los usuarios afectados por el ACE lo son en dos aspectos: costos económicos y costos sociales. También se debe considerar la pérdida de tiempo que suponen, y que puede entenderse como un costo económico indirecto. Si se multiplica el costo de un mensaje a un receptor por los millones de mensajes distribuidos puede hacerse una idea de la magnitud económica, y del porcentaje mínimo de la misma que es asumido por el emisor. En lo que respecta a los costos sociales del ACE debe considerarse, aparte de la molestia u ofensa asociada a determinados contenidos, la inhibición del derecho a publicar la propia dirección en medios como News o Web por miedo a que sea capturada.

2. **Efectos en los operadores.**

Los operadores de destino y encaminamiento acarrean su parte del costo: tiempo de proceso, espacio en disco, ancho de banda, y sobre todo tiempo adicional de personal dedicado a solucionar estos problemas en situaciones de saturación.

NORMATIVA DE USO DEL SERVICIO DE INTERNET

Art. 1. OBJETIVO:

El servicio de correo electrónico (en adelante correo) consiste en la disponibilidad de una dirección de correo electrónico y de un espacio de almacenamiento de mensajes (en adelante buzón de correo).

El objetivo del servicio de correo es dotar de una herramienta útil para el desarrollo de las labores de estudios, investigación o administración de los funcionarios del Instituto Nacional de Meteorología e Hidrología INAMHI.

ART.-2. ÁMBITO DE APLICACIÓN:

Esta norma regula el uso de los recursos informáticos y telemáticos del servicio de correo en el servidor institucional del INAMHI sin perjuicio de las normas y políticas de seguridad de uso generales y por otras leyes de categoría superior que en su momento puedan aplicarse.

Las condiciones que aquí se exponen pueden ser actualizadas para adecuarlas a nuevas situaciones. En particular los plazos de tiempo o límites de espacio en disco que se citan en el presente documento pueden ser modificados en función de las necesidades del servicio y de su evolución en el tiempo.

ART.- 3. TÉRMINOS Y CONDICIONES DE USO DEL SERVICIO DE CORREO ELECTRÓNICO:

Los términos y condiciones de ésta normativa, tienen el carácter de general, se aplican a todos los servicios proporcionados por el INAMHI, el usuario de una cuenta de correo electrónico se compromete a aceptar y cumplir los siguientes:

- Los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de correo en nuestra Institución.
- Está prohibido facilitar u ofrecer la cuenta de correo personal (la clave de acceso al servicio) a terceras personas.
- Se permite usar la cuenta para actividades privadas, actividades no relacionadas con el estudio e investigación o gestión administrativa del INAMHI siempre que no interfieran con el objetivo principal de esta normativa.
- Debe ser consciente de los términos, prohibiciones y perjuicios indicados en el documento "Abuso en el Correo Electrónico".
- Está prohibida la utilización en nuestras instalaciones de cuentas de correo de otros proveedores de Internet.
- No se permite utilizar como encaminador de correo otras máquinas que no sean las puestas a disposición por el INAMHI.
- No se permite enviar mensajes con direcciones no asignadas por los responsables del INAMHI y en general es ilegal manipular las cabeceras de correo electrónico saliente.
- El correo electrónico es una herramienta para el intercambio de información entre personas, no es una herramienta de difusión masiva e indiscriminada de información. Para ello existen otros canales más adecuados y efectivos.
- No es correcto enviar correo a personas que no desean recibirlo. Si le solicitan detener ésta práctica deberá de hacerlo. Si el INAMHI recibe quejas, denuncias o reclamaciones por estas prácticas se tomarán las medidas sancionadoras adecuadas.
- Está completamente prohibido realizar cualquier abuso de los tipos definidos en el capítulo 12 "Abuso en el Correo Electrónico", además de cualquiera de las siguientes actividades:
    - Utilizar el correo electrónico para cualquier propósito comercial o financiero.
    - No se debe participar en la propagación de cartas encadenadas o participar en esquemas piramidales o temas similares.
    - Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados para nuestra institución.
- Estará penalizado el envío a foros de discusiones (listas de distribución y/o grupos de noticias o sociales) de mensajes que comprometan la reputación del INAMHI o violen cualquiera de las leyes.

Para asegurar un normal funcionamiento del servicio y un uso eficiente de los recursos del sistema de correo el funcionario se compromete a:

- Leer periódicamente su correo.
- Hacer un uso responsable de la opción "dejar mensajes en el servidor" (leave mail on server), vaciando periódicamente su buzón, de forma que su tamaño no sea excesivo.
- Hacer uso de la opción "Avisar durante ausencias" cuando el usuario prevea no poder leer el correo durante un intervalo de tiempo largo.
- Hacer uso de la opción "Redireccionar el correo" cuando el usuario desee recibir el correo en una cuenta alternativa.
- Avisar de cualquier incidencia que pueda surgir y que estime puede afectar al normal comportamiento del servicio

Si, en el ejercicio de sus funciones, el personal informático detecta cualquier anomalía que muestre indicios de usos ilícitos, lo pondrá en conocimiento a la autoridad competente.

En caso de no entender completamente alguno de estos apartados puede enviar un mensaje a la dirección soporte@inamhi.gob.ec solicitando le sea aclarado.

ART.- 4. TIPOS DE CUENTAS DE CORREO ELECTRÓNICO:

a. Cuentas de correo personales

Las usadas por funcionarios pertenecientes a alguno de los siguientes segmentos:

- Personal técnico.
- Personal Administrativo y de servicios
- Contratados

El responsable de una cuenta de correo personal es el titular (usuario) de la misma. Sólo se permite una cuenta de correo personal por persona.

b. Cuentas de correo no personales

Además, de las cuentas de correo personales los responsables de las distintas áreas organizativas del INAMHI, podrán solicitar cuentas de correo no personales siempre que estén justificadas y sean necesarias para el normal funcionamiento del área.

Las cuentas de correo no personales estarán vinculadas a una unidad organizativa, siendo el coordinador de dicha unidad el responsable de la cuenta.

Cuando las circunstancias lo requieran, el coordinador de la unidad podrá delegar el uso de la cuenta de correo no personal a una o más personas, siempre que tengan relación formal con el INAMHI y realicen labores dentro de la unidad en cuestión. La delegación se hará efectiva en el mismo momento en que el coordinador de la unidad comunique la clave de acceso al servicio al resto de usuarios de la cuenta. A partir de este momento la responsabilidad sobre el uso de dicha cuenta de correo será conjunta, del coordinador de la unidad y de las personas en quien delega. Queda a criterio del coordinador de la unidad el formalizar mediante escrito o cualquier otro medio la cesión en el uso de la cuenta de correo.

Las cuentas de correo no personales no pueden ser usadas bajo ningún concepto para otros fines que no sean los propios de la unidad a la que pertenece y que motivaron su creación.

En último término será la autoridad competente del INAMHI la que decidirá a qué unidad organizativa pertenece cada una de las direcciones no personales ya existentes del INAMHI, si procede su eliminación o si procede su mantenimiento.

c. Alias

Un alias es una dirección de correo que agrupa a una o más cuentas de correo. A diferencia de una cuenta de correo, los alias no tienen buzón ni clave para acceder al mismo. Los alias se usarán para:

- Redirigir el correo a la dirección nueva en los casos en los que se proceda a cambiar el nombre de una dirección de correo antigua.
- Crear listas de correo.
- Crear direcciones de correo no personales que agrupen a una o más direcciones de correo.

Siempre que las circunstancias lo aconsejen prevalecerá la creación de direcciones de correo no personales mediante alias antes que mediante cuentas de correo. A diferencia del resto de cuentas de correo electrónico, los alias no permiten autenticar el envío de mensajes de correo electrónico.

Los criterios y normas aplicadas a los alias son los mismos que los indicados arriba para las cuentas de correo.

d. Formato de las cuentas de correo electrónico institucionales del INAMHI

Las cuentas de correo electrónico gestionadas por GDI se componen de un nombre (login) y de un dominio de correo y se ajustarán a uno de los dos siguientes formatos:

- xxxxxxxx@inamhi.gob.ec: cuentas de correo no personales y cuentas de correo personales del INAMHI.

Donde xxxxxxxx es el identificativo (login) de la cuenta de correo, y @inamhi.gob.ec es el dominio de correo. El identificativo estará conformado por el primer carácter del nombre más el apellido, en el caso de existir nombres y apellidos comunes, se tomará también el primer carácter del segundo apellido.

Salvo causas justificadas, no se permite cambiar el login de la dirección de correo electrónico. En caso de que el cambio de login se produzca, es responsabilidad del usuario informar del cambio de su dirección de correo a las personas o sistemas a los que les coste la dirección antigua; así como cambiar la antigua dirección por la nueva en cualquier documento en el que conste la antigua, sea cual sea el soporte físico del documento (papel, electrónico, magnético, etc.) No obstante, GDI se compromete a reencaminar el correo dirigido a la antigua cuenta de correo a la cuenta de correo nueva durante el plazo indicado en el parámetro "antigüedad máxima de una dirección de correo a extinguir".

Una vez cumplido el plazo, los mensajes que sigan llegando a la dirección antigua serán rechazados con un código de error "usuario desconocido".

e. Operación del servicio

- **Creación de cuentas de correo electrónico**

Cuentas de correo personales

Existen dos condiciones para crear una cuenta de correo personal:

- El usuario de la cuenta debe ser funcionario del INAMHI.
- Tener una relación de dependencia con el INAMHI.

Cuentas de correo no personales

El solicitante de la cuenta debe estar autorizado para obtener una cuenta de correo no personal. Normalmente estarán autorizados de oficio los responsables de cada unidad organizativa: coordinadores o líderes.

La autoridad competente del INAMHI, en cualquier caso, qué personas están autorizadas para solicitar y obtener cuentas de correo no personales independientemente del cargo que ocupen.

Procedimiento de creación de las cuentas de correo

Siempre que sea posible, la solicitud de creación de la cuenta de correo se efectuará por medios informáticos, para ello el solicitante de la cuenta deberá acreditar su identidad mediante solicitud a la Dirección de Talento Humano.

Una vez comprobada la identidad del solicitante y el derecho a obtener una cuenta de correo, se procederá a la creación de la cuenta. La creación de la

cuenta puede postergarse por motivos técnicos justificados, en cualquier caso GDI informará al solicitante por los medios que considere más conveniente de:

- Cuándo ha sido o será creada la cuenta.
- La clave de acceso a la misma.
- Parámetros de configuración para usar la cuenta de correo.
- Normativa general de uso del servicio de correo.

f. **Estados de las cuentas de correo**

Se tienen en cuenta los siguientes estados en una cuenta de correo:

- ***Activa***: una cuenta de correo está activa cuando puede enviar y recibir mensajes con normalidad.
- ***Bloqueada***: una cuenta de correo está bloqueada cuando no puede enviar o recibir mensajes. Las causas que motivan el bloqueo de una cuenta de correo puede ser alguna de las siguientes:
  - Por decisión de las autoridades del INAMHI (por comisión de infracciones graves o muy graves) o por requerimiento legal.
  - Por haberse llenado su buzón. En este caso la cuenta permanece bloqueada hasta que el usuario de la misma no borra mensajes del buzón.
  - Por detectarse un flujo anormal de mensajes, con esa dirección de correo como destino o como origen, que repercuta en el normal funcionamiento del servicio.
  - Por cualquier otra causa que lo aconseje.
  - El bloqueo de una cuenta de correo puede producirse sólo en la recepción de mensajes, sólo en la emisión o en ambos sentidos.
- ***Abandonada***: se considera que una cuenta de correo está abandonada cuando no tiene redirigido su correo y se ha excedido el "tiempo máximo de inactividad de una cuenta de correo".
- ***Cancelada***: a efectos prácticos para el usuario una cuenta de correo cancelada es una cuenta de correo eliminada. Los mensajes dirigidos a una cuenta de correo cancelada se rechazan con un código de error de "usuario desconocido". El buzón de una cuenta de correo desactivada podrá ser eliminada definitivamente o bien traspasada a un medio de almacenamiento secundario, pero en ningún caso el usuario podrá acceder al mismo.

En cualquier caso, GDI se compromete a avisar con antelación al usuario de una cuenta de correo cuando se prevea un cambio de estado en su cuenta de forma que el usuario pueda adoptar las medidas oportunas que eviten su bloqueo o cancelación.

g. **Cancelación de cuentas de correo**

Se procederá a cancelar una cuenta de correo cuando:

1. La cuenta permanezca abandonada durante un tiempo que exceda el marcado para su cancelación.
2. Por decisión de la autoridad competente del INAMHI por comisión de infracciones que lleven pareja la eliminación de la cuenta de correo.
3. El responsable de la cuenta solicita la eliminación de la misma, siempre que esto no repercuta negativamente en el normal funcionamiento del INAMHI.

En cualquier otro caso será la autoridad competente o el área de Talento Humano del INAMHI la que decida, cuándo y cómo se cancela una cuenta de correo, así como la de arbitrar excepciones a las normas de carácter general arriba expuestas.
Salvo indicación expresa de la autoridad competente del INAMHI, o causas de fuerza mayor, la cancelación de una cuenta de correo será avisada con tiempo suficiente para que el responsable de la misma efectúe las acciones oportunas sobre los mensajes almacenados en su buzón antes de que éstos sean definitivamente eliminados o movidos. El aviso se efectuará mediante mensaje de correo electrónico o por cualquier otro medio que se estime oportuno.
GDI no se responsabiliza de los perjuicios ocasionados por la eliminación de una cuenta de correo y de los mensajes de su buzón en las condiciones arriba expuestas.

La eliminación de una cuenta de correo supone la baja en todos o parte de los servicios citados más arriba.

h. **Gestión del buzón de correo electrónico**

GDI efectuará un control de los siguientes parámetros relacionados con el uso del correo electrónico:

- Estado de los mensajes: nuevo, ya leído, marcado para borrar, respondido, fecha de recepción, etc.
- Tamaño del buzón (espacio total ocupado por los mensajes).
- Fecha del último acceso al buzón del usuario.

La gestión del servicio de correo electrónico, se cuantifica los límites y parámetros que afectan a la gestión de buzón del usuario. Estos límites y parámetros podrán ser modificados en función de las necesidades y evolución del servicio de correo electrónico. GDI avisará a sus usuarios de cualquier modificación que pudiese efectuarse en este sentido. A fin de garantizar un correcto funcionamiento del servicio de correo electrónico, evitando el derroche de recursos y optimizando el rendimiento del sistema, GDI procederá del siguiente modo a la hora de gestionar el espacio dedicado a almacenar los mensajes de correo de cada usuario:

1. Una vez alcanzado el tamaño máximo del buzón no se podrán recibir más mensajes en el buzón hasta que el usuario no borre mensajes del mismo. En estos casos también se podrá restringir el envío de mensajes.
2. Si se alcanza el tiempo máximo de inactividad de una cuenta de correo (cuenta de correo abandonada) se procederá a eliminar la suscripción de la cuenta de correo la dirección de correo de las listas de correo del INAMHI a las que pudiera estar suscrita.

En cualquier caso GDI se compromete a avisar con la antelación suficiente y por los medios oportunos al usuario afectado antes que se dé alguna de las situaciones contempladas arriba.

i. **Mantenimiento del servicio**

GDI se reserva el derecho a cambiar cualquier parámetro de configuración del servicio de correo con el fin de incorporar mejoras, monitorizar el servicio, restringir accesos, etc. GDI se reserva el derecho de parar el servicio cuando las circunstancias lo requieran; si se prevé una parada larga GDI avisará con antelación enviando un mensaje a todos los usuarios de correo.

Cuando las circunstancias impidan avisar a los usuarios con antelación suficiente y la parada se prolongue durante más tiempo del deseado, GDI informará a posteriori de los motivos de la parada.

***j.* Gestión de incidencias**

Cualquier incidencia que afecte a un usuario del INAMHI debe gestionarse a través del sistema.

Las incidencias que supongan quejas o consultas de personas o entidades ajenas al INAMHI se encauzarán a través de alguna de las siguientes direcciones de correo:

- postmaster@inamhi.gob.ec: administrador del servicio de correo del INAMHI.
- abuso@inamhi.gob.ec: para dirigir consultas y quejas sobre incidentes originados en el INAMHI.
- antivirus@inamhi.gob.ec: para dirigir consultas y quejas sobre virus propagados por correo electrónico

***k.* Copias de seguridad**

GDI se compromete a realizar copia de seguridad de los siguientes aspectos del servicio de correo electrónico:

- Programas y archivos de configuración del propio servicio
- Archivos de registro de eventos o "logs"
- Buzones de los usuarios de correo.
- Archivos de configuración personales de los usuarios depositados en el servidor

La frecuencia y número de copias de seguridad efectuadas podrán variar en función de la disponibilidad y características de los datos a almacenar. En cualquier caso, GDI no asegura la recuperación de mensajes eliminados a partir de las copias de seguridad de los buzones. Es responsabilidad del usuario del buzón el efectuar copia de los mensajes que considere importantes en un medio local y personal: disco duro, disquete, CD-ROM, etc.

***l.* Supervisión y monitorización**

GDI, podrá monitorizar, intervenir y examinar el contenido de los mensajes y buzones de los usuarios en alguna de las siguientes circunstancias:

- Cuando el responsable de la cuenta de correo lo pida, para detectar y corregir posibles problemas que afecten al normal funcionamiento de la cuenta.
- Cuando sucedan eventos que afecten al funcionamiento general del servicio, para detectar el origen y las causas del problema.
- Cuando la autoridad competente del INAMHI lo solicite.
- Por requerimiento legal.

***m.* Registro de eventos**

GDI registra en archivos específicos el funcionamiento y uso del correo electrónico. En concreto se generan trazas de los siguientes eventos:

- Envío y recepción de mensajes.
- Acceso a los buzones de los usuarios.
- Alta, baja, modificación y consulta de cuentas de correo.
- Cambios de claves de acceso al buzón.
- Cambios en archivos de configuración personales de los usuarios.

Para cada uno de estos eventos se registra de manera detallada todos los datos concernientes al mismo: direcciones IP de los ordenadores, direcciones de correo del remitente y del destinatario, etc.

En el futuro podrán registrarse nuevos eventos relativos al servicio de correo electrónico.

***n.* Estadísticas del servicio**

GDI generará estadísticas del servicio de correo con el fin de medir su rendimiento, el uso que se hace del mismo y detectar o prevenir posibles comportamientos anómalos que pudieran producirse. Parte de las estadísticas podrán hacerse públicas para información de las autoridades.

En la medida de lo posible se generarán estadísticas de uso personal del correo para cada cuenta, las cuales sólo serán accesibles por el responsable de la cuenta.

ñ. Detección y eliminación de virus

El correo electrónico es uno de los medios de difusión de virus más importantes. Para prevenir la propagación masiva de virus y gusanos informáticos, se aplican las siguientes medidas sobre todos los mensajes que entran o salen del INAMHI, así como sobre el correo interinstitucional que tenga como origen o destino alguno de las direcciones de correo gestionadas por GDI:

- No se permiten mensajes de correo con anexos ejecutables o susceptibles de contener código malicioso.
- Si se desea enviar un mensaje con un anexo ejecutable, sólo podrá hacerse si previamente se comprime en algún formato conocido (.zip, .gzip, etc.)
- Los mensajes serán examinados por un programa antivirus, de forma que se garantice, en la medida de lo posible, que los mensajes que entran y salen del INAMHI están limpios

El procedimiento utilizado a la hora de detectar un mensaje con código malicioso en un anexo es el siguiente:

- Nunca se envía un mensaje de aviso al remitente del mensaje, pues la mayoría de mensajes infectados son generados por gusanos que falsifican la dirección de correo del remitente.
- En el caso de que el mensaje haya sido generado por un gusano, el mensaje se descarta y no se entrega a los destinatarios.
- Si se puede eliminar el virus del anexo se elimina y se entrega el mensaje a los destinatarios con el anexo libre de virus. En el mensaje se incluye un literal avisando del evento e indicando el tipo de virus eliminado.
- Si no se puede eliminar el virus del anexo se entrega el mensaje a los destinatarios sin el anexo. En el mensaje se incluye un literal avisando del evento e indicando el tipo de virus eliminado.

ART. 5. DETECCIÓN Y CONTROL DE PCS INFECTADOS Y MENSAJES GENERADOS POR LOS MISMOS:

La detección de PCs infectados se realiza inspeccionando las cabeceras de los mensajes infectados, a partir de la dirección IP de origen del mensaje. A fin de minimizar la propagación de gusanos y virus (sobre todo cuando son de reciente aparición y los programas antivirus no logran detectarlos), GDI podrá

ejecutar todas o algunas de las siguientes acciones sobre los equipos infectados o mensajes generados desde los mismos:

- Desactivar el punto de red al que está conectado el equipo.
- No permitir el tráfico SMTP con origen en el equipo.
- Rechazar en la estafeta de salida del INAMHI los mensajes generados desde ese equipo.
- Rechazar los mensajes que se ajusten a un determinado patrón en la cabecera o en el cuerpo.

El usuario responsable del equipo afectado será informado del hecho tan pronto como sea posible para que proceda a la desinfección del equipo, al tiempo que personal de GDI se pondrá a su disposición para dicha tarea. Una vez limpio el equipo, se procederá a restituir los servicios que pudieran haber sido desactivados.

ART. 6. RESPONSABILIDADES ASOCIADAS A LA PROPAGACIÓN DE VIRUS:

GDI declina cualquier responsabilidad derivada de la propagación de virus y gusanos a través del correo electrónico, siendo responsabilidad del usuario el tomar las medidas necesarias para evitar la infección y sus consecuencias; entre las medidas se incluyen:

- No abrir ficheros adjuntos en mensajes de correo no solicitados aunque procedan de remitentes conocidos.
- Usar un antivirus en el ordenador personal y mantenerlo actualizado.
- Efectuar copias de seguridad periódicas de los programas, datos y configuraciones de su equipo.

a. Detección y eliminación de correo basura (spam)

Para minimizar la llegada de correo basura a los buzones de los usuarios se aplicarán todas o parte de las siguientes medidas sobre todos los mensajes que entran o salen del INAMHI, así como sobre el correo interinstitucional que tenga como origen o destino alguno de las direcciones de correo gestionadas por GDI. Las medidas se categorizan según distintos criterios:

Control de la procedencia y destino de los mensajes

- Uso de listas negras para el rechazo sistemático de mensajes provenientes de estafetas mal configuradas o "abiertas".
- Uso de listas blancas para posibilitar la inclusión de excepciones a las listas negras.
- Uso de listas grises para evitar el spam generado desde programas especializados.
- Impedir el envío de mensajes con direcciones de correo falsificadas.
- Uso de filtros en la estafeta: rechazar estafetas no registradas en el DNS, sin resolución inversa o sin registros MX, etc.
- Autenticación de los remitentes de mensajes.
- Autenticación de las estafetas intermedias.
- Uso de cualquier otro mecanismo de nueva aparición y que sea útil al propósito que nos ocupa.

b. Control del flujo de mensajes

Tienen como objetivo detectar patrones de tráfico de correo desde y hacia el INAMHI anómalos, sospechosos de constituir ataques de spam. Cuando se detecta un flujo de mensajes de este tipo los mensajes no se entregan inmediatamente, sino que se almacenan para su posterior inspección. Si se comprueba que los mensajes son correo basura se eliminan, si no lo son se entregan normalmente.

c. Análisis del contenido de los mensajes

Se inspeccionan las cabeceras y los contenidos de los mensajes y se calcula la probabilidad de que se trate de un mensaje de spam o no. Si el mensaje se considera spam, se marca para que el receptor del mismo pueda distinguirlo del resto de mensajes. Si no se considera spam el mensaje se entrega normalmente.

d. Responsabilidades asociadas a la detección y eliminación de spam

GDI declina cualquier responsabilidad derivada de la aplicación de las medidas arriba expuestas.

El usuario de correo del INAMHI acepta las medidas arriba expuestas y cualquier otra que pueda ser adoptada en el futuro, tendientes a reducir el tráfico de correo basura desde y hacia el INAMHI.

El usuario de correo debe ser consciente de que la aplicación de las medidas arriba expuestas puede dar lugar a las siguientes situaciones:

- Rechazo sistemático de mensajes provenientes de estafetas mal configuradas.
- Rechazo sistemático de mensajes dirigidos a estafetas mal configuradas.
- Generación de falsos positivos: mensajes marcados como spam que no los son.
- Generación de falsos negativos: mensajes no marcados como spam que sí lo son.
- Retardos en la entrega o recepción de mensajes de correo.

En cualquier caso GDI se compromete a tomar las medidas necesarias para minimizar estos casos. Por su parte, el usuario de correo se compromete a avisar al personal informático de cualquier indicio o problema que pudiera acontecer relativo a la detección y eliminación de spam.

e. Identidad del usuario de correo electrónico

El usuario debe identificarse mediante su clave de acceso al correo siempre que se le solicite, en particular para acceder a su buzón. La solicitud de clave podrá ampliarse en cualquier otra circunstancia que en el futuro se considere necesaria.

Es obligación del usuario configurar adecuadamente su programa de correo para:

- Identificarse correctamente ante el servicio cuando éste lo requiera.
- Que su nombre y apellidos (en el caso de cuentas de correo personales) o la descripción de la cuenta (en el caso de cuentas de correo no personales) aparezca en las cabeceras de los mensajes que envíe.

En cualquier caso, GDI no garantiza que la identidad aparecida en las cabeceras de un mensaje de correo se corresponda con la identidad real del usuario que envió el mensaje (limitación del protocolo SMTP de transferencia de mensajes de correo electrónico). Para salvar esta situación GDI permitirá que los mensajes enviados desde cuentas personales sean firmados mediante un certificado digital personal del usuario, de manera que el destinatario del mensaje pueda comprobar la identidad del remitente. Es responsabilidad del usuario configurar adecuadamente su programa de correo para comprobar este hecho.

f. Confidencialidad del servicio de correo electrónico

El responsable de una cuenta de correo electrónico se compromete a no develar su clave de acceso (salvo en los casos en que delegue su uso), así como a elegir una clave suficientemente segura que impida que terceros puedan adivinarla mediante técnicas de "fuerza bruta" o similares.

En este sentido GDI pondrá los medios necesarios para que los usuarios de correo usen claves seguras, en particular:

- Forzará la elección de claves seguras durante los procesos de solicitud y creación de cuentas y durante el proceso de cambio de clave.
- Efectuará controles periódicos de las claves de sus usuarios, pudiendo obligar a cambiar claves de correo "débiles" a los usuarios que las tuviesen.

Por su parte, GDI se compromete a poner los recursos necesarios para permitir encriptar las claves de sus usuarios cuando circulen por la red; la encriptación se hará extensible al contenido de los mensajes cuando el usuario así lo solicite.

Es responsabilidad del usuario el configurar adecuadamente su programa de correo para solicitar los servicios de encriptación del correo. GDI se compromete a ofrecer los mecanismos y la documentación necesaria para facilitar esta tarea.

g. Integridad de los mensajes de correo

Con objeto de garantizar la integridad de los mensajes de correo, GDI pondrá a disposición de sus usuarios una infraestructura de clave pública y privada que permita efectuar un "hash" de los mensajes enviados y un posterior chequeo de la integridad por parte del destinatario de los mensajes.

h. Limites y parámetros de gestión del servicio de correo electrónico

Con carácter general se aplican los siguientes limites y parámetros a la hora de gestionar el servicio de correo electrónico:

Tamaño máximo del buzón	100 MB
Tiempo máximo de inactividad de una cuenta de correo (cuenta de correo abandonada)	270 días
Antigüedad máxima de una dirección de correo a extinguir	90 días

Los límites y parámetros pueden ser modificados en cualquier momento, así como ser definidos nuevos límites y parámetros. GDI informará de cualquier cambio efectuado en este sentido.

NORMATIVA PARA USO ACEPTABLE DE INTERNET EN EL INAMHI

Art.1.OBJETIVO:

Los funcionarios del INAMHI tienen a su disposición servicios informáticas entre los cuales está el servicio ilimitado de Internet, correo electrónico (e-mail), navegación y otros, archivos o cuentas de la red informática. La meta al proveer el acceso a Internet a los mismos, es promover la eficiencia y excelencia en el lugar de trabajo, facilitando compartir la información, la innovación, la comunicación, la cooperación y la colaboración.

ART.2. ALCANCE TÉCNICO:

El acceso al Internet está coordinado a través de una conexión de línea dedicada tipo ADSL de 8 Mbps de ancho de banda. El acceso mundial a las computadoras y otras personas puede involucrar como consecuencia la posibilidad de obtener material considerado inapropiado, ilegal o de ningún valor educativo. En una red global es prácticamente imposible controlar todo el material. Sin embargo, a través de un sistema de depuración y monitoreo, la unidad de Gestión de Desarrollo Informático ha tomado precauciones para restringir el acceso a material inapropiado.

El funcionamiento regular de la red, depende de la conducta apropiada de los usuarios, quienes deben regirse a normas, reglas y reglamentaciones. Las mismas se proveen para que los usuarios estén conscientes de las responsabilidades que están a punto de aceptar. En general sus responsabilidades incluyen el uso eficiente, ético y legal de los recursos de la Internet.

ART 3. TÉRMINOS Y CONDICIONES DE USO:

1. **Privilegios:** El uso de la Internet es un privilegio, no un derecho. El uso inapropiado de la misma puede resultar en una solicitud de acción disciplinaria. El responsable de la Unidad de Gestión de Desarrollo Informático o el administrador de sistemas de dicha unidad, puede limitar, suspender o revocar el acceso a los recursos de la Internet en cualquier momento.
2. ***Uso aceptable:*** El uso de una cuenta asignada debe ser para asistir la investigación; y/o dentro de las metas, funciones, responsabilidades y objetivos institucionales, profesionales o metas personales de trabajo atinentes a la unidad técnica correspondiente.
   La transmisión o recepción intencional de material inapropiado o de material en violación con la ley, está prohibida. Esto incluye, pero no se limita a: materiales con derechos de autor; material con amenazas u obsceno; material protegido por secretos comerciales; el diseño o información detallada de dispositivos explosivos; actividades criminales o actos terroristas; discriminación o acoso sexual; pornografía; juegos de azar; solicitación ilegal; racismo; lenguaje inapropiado; uso para la publicidad de un producto; o propaganda política.
   Cualquier funcionario que "publica" en la Internet, debe regirse por los procedimientos aprobados para la publicación, y estas normas, las cuales incluyen informar e involucrar al administrador de la organización en el procedimiento de publicación. Actividades de publicación ilegal o inapropiada, o usos de cualquier tipo que no estén de conformidad con las reglas, reglamentos y normas dispuestas por esta unidad, están prohibidas. Se aconseja no divulgar información personal tal como: dirección de su casa, números de teléfono, códigos (passwords), números de tarjetas de crédito; esto también se aplica para la información personal de otros individuos u organizaciones.
3. ***Ética en el uso de Internet:*** Los funcionarios del INAMHI tienen la responsabilidad de asegurarse de que toda la información compartida cumple con las normas establecidas en este Acuerdo de Uso Aceptable. Se espera que cada poseedor de una cuenta se rija por las reglas de ética para el usuario aceptadas generalmente. Estas reglas incluyen, pero no se limitan a lo siguiente:
   a. Sea cortés. Nunca envie o aliente a otros a enviar mensajes abusivos. Use lenguaje apropiado. No se garantiza que el correo electrónico (e-mail) sea ciento por ciento privados. Todo lo que se escribe, envía o se recibe en una terminal individual tiene la posibilidad de ser visto globalmente.
   b. No use la red Internet de ninguna manera que pueda interferir con el uso de la misma por otros. Utilice los recursos en forma apropiada, lo cual incluye no usarla para ventas, publicidad o solicitaciones. Mensajes relacionados a, o en apoyo de, actividades ilicitas o inapropiadas (según este Acuerdo de Uso Aceptable), deben ser denunciadas al responsable apropiado o al administrador de sistemas de la unidad.
4. ***Vandalismo:*** Se define al vandalismo como cualquier intento malicioso para dañar o destruir la propiedad del mismo usuario, de otro usuario o de cualquier área o red que esté conectada a la red informática o al sistema de Internet. Vandalismo también incluye, pero no se limita a: sobrecargar datos; ingresar, descargar o crear un virus de computadora.
5. ***Seguridad:*** La seguridad en cualquier sistema de computadoras es de alta prioridad por causa de los múltiples usuarios. No use la cuenta de otro individuo ni entre al sistema como un administrador de sistemas. Se debe informar inmediatamente al responsable o al administrador de sistemas de la unidad de Gestión de Desarrollo Informático sobre cualquier inquietud en cuanto a la seguridad.
6. ***Negación de responsabilidad por el servicio:*** La unidad de Gestión de Desarrollo Informático no garantiza de ninguna manera, ya sea en forma explícita o implícita, los servicios que provee. La unidad de Gestión de Desarrollo Informático no será responsable por daños que el funcionario/a pueda sufrir usando el sistema. Estos daños pueden incluir, pero no se limitan a: pérdida de datos como resultado de demoras, información no transmitida, información mal transmitida, interrupciones en el servicio causadas por el sistema o por error u omisión del funcionario. El uso de la información obtenida por vía del sistema de información es al riesgo exclusivo del funcionario/a. La unidad de Gestión de Desarrollo Informático declina especificamente toda responsabilidad por la exactitud de la información obtenida a través de los medios informáticos.

NORMATIVA PARA EL USO DE INTERNET

Art. 1. DE LA FINALIDAD DE ESTA NORMATIVA:

Esta normativa, tiene por finalidad regular el uso del Internet, por parte de los funcionarios del INAMHI y de todas aquellas personas particulares y miembros de instituciones que, por convenios establecidos con esta Institución, obtienen acceso al servidor de la misma (por Ej. Pasantes, tesistas, comisión de servicios), por medio de cuentas de correo electrónico, WWW (World Wide web), trasferencias de archivos, y toda forma de tecnología que se desarrollare en el futuro dentro de la Internet.

ART. 2. DE LOS USUARIOS

Tienen acceso al uso del servicio de Internet del INAMHI:

- El Director Ejecutivo del INAMHI y los Señores Directores Técnicos de Área.
- Los funcionarios a nombramiento.

Tienen derecho a solicitar acceso al uso del servidor del INAMHI:
Coordinadores y líderes, así como el resto de funcionarios, siempre que lo soliciten con el respaldo escrito de la autoridad pertinente (visto bueno), en nota dirigida a la Unidad de Gestión de Desarrollo Informático del INAMHI y la conexión sea factible en relación al ancho de banda contratado.

ART. 3. DE LA AUTORIZACIÓN PARA SER USUARIO:

El responsable de la Unidad de Gestión de Desarrollo Informático está facultado para aceptar o rechazar las solicitudes para convertirse en usuario autorizado de la red, fundamentando tal rechazo. Así mismo, puede suspender temporal o definitivamente la autorización. La suspensión definitiva importará la presentación de un informe al Director de Gestión de Desarrollo Organizacional y Director Ejecutivo del INAMHI para su tratamiento.

ART. 4. DE LA DURACIÓN DE LA AUTORIZACIÓN:

La duración de la autorización se extenderá ordinariamente durante el tiempo en que el usuario se mantenga legalmente en la Institución, cumpliendo el rol que justificó tal autorización, sin perjuicio de su sometimiento a las políticas y normas que para el efecto establecieren el Responsable de la unidad de Gestión de Desarrollo Informático y a la disposición de los recursos necesarios.

ART. 5. DEL RECONOCIMIENTO DE LA RESPONSABILIDAD DEL USUARIO:

Cada usuario, se da por enterado de estas reglas desde el momento que es considerado como tal por la unidad de Gestión de Desarrollo Informático derivando la correspondiente responsabilidad por sus acciones, al acceder al Internet, a través del servidor del INAMHI.

ART. 6. DE LAS SANCIONES:

El acceso al servidor del INAMHI es una concesión que puede ser revocada en cualquier momento, si se detecta uso indebido o acción que contradiga lo dispuesto en el Art. 7 de esta normativa. Cualquier violación de las normas de este reglamento puede resultar en la revocatoria temporal o permanente del acceso al servidor, sin perjuicio de las sanciones contempladas en las normas institucionales y en la Ley.
Las infracciones leves serán juzgadas y sancionadas el Líder de la unidad de Gestión de Desarrollo Informático, previo informe del Administrador de la Red (de Internet). Las infracciones graves serán juzgadas y sancionadas por el Director de Gestión Organizacional y el Director Ejecutivo, previo informe del Responsable de la Unidad de Gestión de Desarrollo Informático.

ART. 7. DE LAS NORMAS ÉTICAS QUE RIGEN EL USO DE LA RED:

Es responsabilidad grave de cada usuario utilizar la Internet de acuerdo a la ética y a las leyes y reglamentos pertinentes; por lo tanto:

- Todo mensaje enviado por un usuario debe incluir su identificación y dirección electrónica.
- Está prohibido poner información ilegal en un sistema. Se entiende por información ilegal aquella obtenida o manipulada sin el consentimiento de su propietario.
- Está prohibido el uso de lenguaje inapropiado u ofensivo, en mensajes privados o públicos.
- Está prohibido el uso del servidor para fines no identificados con la misión de la Institución y con la optimización de la eficiencia administrativa de la misma.
- Está prohibido cualquier uso del servidor para negocios particulares o actividades no relacionadas con las funciones del puesto, o para el beneficio particular de terceras personas o de instituciones que no tengan autorización o acuerdos con el INAMHI, o para cualquier finalidad que no concuerde con el espíritu de esos acuerdos.

ART. 8. DE LAS RECOMENDACIONES Y PROHIBICIONES PARA EL USO DE LA RED DE INTERNET EN LA INSTITUCIÓN

El usuario de la Internet debe colaborar responsablemente en la utilización eficiente de los servicios y recursos que la Institución pone a su disposición. Por tanto, la inobservancia ocasional de las siguientes recomendaciones será considerada como una falta leve, pero su reincidencia será causal de sanciones inclusive severas, de acuerdo a la gravedad de los perjuicios que cause a la Institución, a las personas o a la eficiencia en el uso de la red. Pudiendo ser posible de corte en la provisión de señal de forma momentánea o definitiva.

Por lo tanto, se recomienda:

- Cambiar periódicamente su clave de acceso (password) de su correo electrónico.
- Revisar su correo electrónico diariamente o, al menos, una vez por semana; grabar la información necesaria en carpetas de archivo y borrar inmediatamente los mensajes no deseados para mantener al mínimo el número de mensajes que queden en el buzón electrónico, a fin de no sobrecargar la capacidad de almacenamiento en disco del servidor de mail. En consecuencia, el Administrador del Sistema de la unidad de Gestión de Desarrollo Informático eliminará todo mensaje adicional a los 30 últimos recibidos o a un espacio de utilización superior a los 500 K bytes, sin responsabilidad por la pérdida de la información.
- Borrar de su directorio los archivos que no necesite y/o comprimir los que use con poca frecuencia.
- Evitar la transferencia innecesaria de archivos, especialmente cuando su tamaño es de mucha capacidad. Cuando sea necesario transferir archivos grandes, hacerlo fuera de las horas laborables.
- Si se requiere de un software disponible en la red, cuyo tamaño exceda los 4 megas se comunicará a la unidad de Gestión de Desarrollo Informático para solicitar instrucciones del momento más oportuno para hacerlo, de modo tal a no saturar el ancho de banda del cual dispone la Institución.
- Conocer y respetar las políticas y procedimientos de cada red a la que accede, pues el hecho de que un usuario esté en capacidad de ejecutar una acción en particular no implica que esté autorizado para hacerla.
- Especialmente, revisar las licencias y permisos para copiar software y, en caso de duda, evitar hacerlo y consultar con el personal de la unidad de Gestión de Desarrollo Informático.
- Respetar el orden regular al dirigir correspondencia a las autoridades.
- No interferir con la dedicación de los usuarios a sus actividades laborales, utilizando herramientas como correo electrónico -que no sea el institucional-, chats, mensajeros, reproductores de Mp3, etc.

PROHIBICIONES:

- Queda terminantemente prohibido bajar archivos musicales del tipo mp3, mp4, wmv o wav, así como archivos de películas en cualquier formato.

- Crear conexiones paralelas (vía proxy), a usuarios que no estén autorizados y/o sin consentimiento de la unidad de Gestión de Desarrollo Informático.
- Cambiar las configuraciones originales dejadas por los técnicos de la unidad de Gestión de Desarrollo Informático.
- El uso de ftp, telnet, finger, etc. sin autorización y conocimiento de la unidad de Gestión de Desarrollo Informático.

ART. 9. DE LA INTERPRETACIÓN Y APLICACIÓN DE ESTA NORMATIVA

El Director de Gestión de Desarrollo Organizacional y el Director Ejecutivo, en orden de jerarquía los casos no contemplados en esta normativa o que requieran la interpretación del mismo, pudiendo delegar dicha interpretación al Líder de la Unidad de Gestión de Desarrollo Informático del INAMHI.

NORMATIVA PARA USO ADECUADO DE SOFTWARE Y HARDWARE DEL INAMHI

Art. 1. OBJETIVO:

La presente normativa, tiene como objetivo, estandarizar el uso y administración de las Computadoras asegurar que los recursos humanos y tecnológicos comprometidos en la obtención de la información, sean acordes con las inversiones que la Institución realiza.

- Los usuarios de los Computadores serán responsables de cumplir y hacer cumplir las normas y procedimientos aquí expuestos.
- Cuando haya necesidad de modificar, adicionar o suprimir las normas o procedimientos presentes, la unidad de Desarrollo Informático remitirá a la Dirección de Desarrollo Organizacional el Proyecto, con el fin que este determine la concordancia de las nuevas normas y procedimientos, con los demás de la Institución, para no alterar el sentido y enviarlos a los usuarios.

ART. 2. ADQUISICIÓN Y USO DE SOFTWARE Y HARDWARE

1. Software

En términos generales se puede definir que el Software es un conjunto de programas para llevar a cabo un objetivo específico y a su vez un programa es un conjunto de instrucciones que realizan una tarea para cumplir dicho objetivo. El software para Computadores se puede clasificar en los siguientes tipos:

- **Sistema operacional**: Es el conjunto de programas que controla las actividades operativas de cada Computadora y de la Red.
- **Paquete de Usuario Final**: Mediante los cuales el usuario de una manera sencilla elabora sus procesos, por ejemplo, hojas de cálculo, manejadores de bases de datos, procesadores de palabras, etc.
- **Paquete de Sistemas Aplicativos**: En los que a diferencia de los anteriores, el usuario es simplemente quien los usa. La programación y el desarrollo es compleja, realizada por la unidad de desarrollo informático o adquiridos a proveedores externos, por ejemplo, sistema de nómina, sistema de contabilidad, sistemas de inventarios, etc.

2. Software Autorizado

Se considera como Software autorizado, tanto los sistemas operacionales como aquellos paquetes de usuario final y de sistemas aplicativos, que la unidad de Desarrollo Informático ha instalado, previo visto bueno para su adquisición y con la autorización legal del proveedor para su uso.

3. Hardware

Hardware es la parte física, tanto interna como externa de un Computador. La selección del modelo y capacidades del hardware requerido por determinada dependencia, debe ir de acuerdo con el plan informático de la unidad de desarrollo informático y sustentado por un estudio elaborado por el mismo, en el cual se enfatizan las características y volumen de información que ameritan sistematización y diferencian los tipos de equipos que se adjudican a las diversas áreas usuarias.

Todo estudio determina una configuración mínima para el computador y los aditamentos o dispositivos electrónicos anexos como unidades externas, impresoras, tarjetas y módems para comunicaciones, elementos para backups en cintas magnéticas, etc.; de acuerdo con las necesidades del usuario, así como una evaluación del costo aproximado de la inversión.

ART. 3. NORMAS SOBRE LA UTILIZACIÓN DE SOFTWARE Y HARDWARE:

- El uso de Software no autorizado o adquirido ilegalmente, se considera como PIRATA y una violación a los derechos de autor.
- El uso de Hardware y de Software autorizado está regulado por las siguientes normas:
  - Toda dependencia podrá utilizar ÚNICAMENTE el hardware y el software que la unidad de Informática le haya instalado y oficializado mediante el "Acta de entrega de equipos y/o software".
  - Tanto el hardware y software, como los datos, son propiedad de la Institución; su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias del INAMHI, será sancionada de acuerdo con las normas y reglamento interno de la Institución. Desarrollo Informático llevará el control del hardware y el software instalado, basándose en el número de serie que contiene cada uno.
  - Periódicamente, desarrollo informático efectuara visitas para verificar el software utilizado en cada dependencia. Por lo tanto, el detectar software no instalado por esta dependencia, será considerado como una violación a las normas internas de la Institución.
  - Toda necesidad de hardware y/o software adicional debe ser solicitada por escrito al departamento de sistemas, quien justificara o no dicho requerimiento, mediante un estudio evaluativo.
  - El departamento de sistemas instalara el software en cada computador y entregara al área usuaria los manuales pertinentes los cuales quedaran bajo la responsabilidad del Jefe del Departamento respectivo.
  - Los disquetes que contienen el software original de cada paquete serán administrados y almacenados por el Departamento de Sistemas.
  - El Departamento de Sistemas proveerá al personal una copia del software original en caso de requerirse la reinstalación de un paquete determinado.
  - Los trámites para la compra de los equipos aprobados por el departamento de sistemas, así como la adecuación física de las instalaciones serán realizadas por la dependencia respectiva.
  - La prueba, instalación y puesta en marcha de los equipos y/o dispositivos, serán realizados por el Departamento de Sistemas, quien una vez compruebe el correcto funcionamiento, oficializará su entrega al área respectiva mediante el "Acta de Entrega de Equipos y/o Software".
  - Una vez entregados los equipos de computación y/o el software por el departamento de sistemas, estos serán cargados a la cuenta de activos fijos del área respectiva y por lo tanto, quedaran bajo su responsabilidad.
  - Así mismo, el departamento de sistemas mantendrá actualizada la relación de los equipos de computación de la Institución, en cuanto al número de serie y ubicación, con el fin que este mismo departamento verifique, por lo menos una vez al año su correcta destinación.
  - El Departamento de Sistemas actualizara el software comprado 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.

ART. 4. MANTENIMIENTO DE EQUIPOS:

a. **Contrato de mantenimiento**

- Con el fin de garantizar un correcto funcionamiento de los equipos de computación (computadores, impresoras y cualquier dispositivo anexo) se debe contar con un contrato de mantenimiento tanto preventivo como correctivo con firmas especializada que presten de una manera rápida y efectiva este tipo de servicio o en su defecto por el departamento interno de servicios.
- El departamento de sistemas controlará y supervisará la garantía de los equipos y dispositivos existentes en todas las dependencias y el contrato de mantenimiento de estos.
- En el caso de existir un mantenimiento contratado debe cubrir, tanto en el tipo preventivo como en el correctivo, el reemplazo de piezas y/o tarjetas defectuosas pierde validez cuando se comprueba que el usuario ha abierto el equipo o tratado de reparar por su cuenta el daño presentado. Se exceptúa de éste cubrimiento, las cabezas de impresión, cuyo costo debe ser asumido por la dependencia usuaria.
- El Departamento de Sistemas mantendrá una hoja de vida de cada equipo, que contemple las revisiones efectuadas, cambios de piezas y modificaciones realizadas y las estadísticas de su rendimiento.

b. **Solicitud de mantenimiento**

- El mantenimiento preventivo de equipos de cómputo se ajusta a un plan trazado por el Departamento de Sistemas y se realizará generalmente cada seis meses sin que se requiera de una solicitud previa del área, con el fin que esta pueda programar sus actividades y entregar los equipos para su mantenimiento.
- Para el mantenimiento correctivo, el usuario del computador deberá comunicarse con el departamento de sistemas, para informarle la falla presentada.
- Al Solicitar un servicio de mantenimiento el usuario debe tener presente los siguientes datos:

  - Dependencia que hace el reporte.
  - Modelo de la computadora, impresora o dispositivo.
  - Número de serie.
  - Código de error o descripción del problema presentado.

ART. 5. SEGURIDAD DE LA INFORMACIÓN:

a. **Protección contra accesos no autorizados**

- La información, como recurso valioso de una organización, está expuesta a actos tantos intencional borrado y copia, por lo que se hace necesario que el usuario, propietario de esa información, adopte medidas de protección contra accesos no autorizados.
- Las siguientes pautas o recomendaciones, ofrecen la posibilidad de habilitar cierto grado de protección con los medios actualmente disponibles en la institución.

b. **Clave de autorización de encendido**

- Este es un recurso de protección disponible en todos los computadores, se habilita al momento de configurar el equipo y es una clave que será solicitada como primer paso de inicialización después de encendido el computador.
- Todo computador, será entregado por el departamento de sistemas con este medio de protección activado, previa autorización del usuario.
- Cuando se activa esta protección se debe tener presente las siguientes consideraciones:

  - No olvide su clave. Su desactivación puede gastar tiempo valioso durante el cual el computador no puede ser utilizado.
  - Dé a conocer la clave sólo a aquellas personas que realmente deben encender y hacer uso del equipo.
  - El sistema exigirá la modificación periódica de su clave.

ART. 6. COPIAS Y/O BACKUPS DE RESPALDO:

- Así como se protege la información contra accesos no autorizados y como complemento a las copias periódicas que cada usuario obtiene de su propia información, es también importante mantener en lugar seguro y externo al sitio de trabajo, copias actualizadas de la información VITAL de cada dependencia, con el fin de garantizar la oportuna recuperación de datos y programas en caso de pérdidas o daños en el computador.
- Las siguientes pautas determinan una buena política de Backups aplicable en cada dependencia de la institución.

  - Determine el grado de importancia de la información que amerite copias de seguridad.
  - Comunique al departamento de sistemas para que este elabore copias periódicas a través de la red.
  - Indique cuanto tiempo se debe conservar esta información.

ART. 7. PROTECCIÓN CONTRA "VIRUS":

- El Virus por computadora puede definirse como un: "programa con capacidad de reproducir un error (infección) e insertarlo en las áreas de datos, de programas y en otras del mismo sistema y alterar su normal funcionamiento". Estos, atacan destruyendo la integridad de la información contenida en los medios de almacenamiento magnético llegando incluso a dañar partes físicas de la máquina.
- Dentro de la infinidad de virus detectados en el mundo entero y fácilmente reproducidos por el uso y copia de software "pirata", utilización de disquetes ya "infectados", o Vía E-Mail. Podríamos destacar los siguientes: Viernes Trece, Abril Primero, Mixer 1, Alabama, Cien años, La Bestia, Miguel Angel, Stoned, Cerebro Pakistani, Mellisa, buddylst.zip, a.i.d.s. Virus, the crew, open:verycool!:, Macros de Word.
- Los componentes que más comúnmente son afectados por los virus son los siguientes:
  - Las tablas de localización de archivos (FATS) que al modificarse ocasiona la pérdida total del contenido del disco duro.
  - La asignación de discos, que al ser modificadas graba la información en el volumen equivocado.
  - Programas y archivos de datos que son removidos (borrados) del disco duro o del disquete.
  - Archivos de datos a los cuales se les altera su longitud y contenido.
  - Espacios libres de almacenamiento que se ven reducidos por la duplicación de programas y/o de archivos de datos.
  - Programas del sistema operacional residentes en memoria que son eliminados o modificados
  - Sectores del disco duro o de disquete que son declarados como defectuosos.
  - Partes lógicas de tarjetas inteligentes las cuales pueden verse afectadas en sus funciones pre programadas.
- Aunque existen tratamientos "vacunas", lo primordial es prevenir el contagio mediante la adopción de una política de "sano" procesamiento que el usuario debe seguir:
  - Utilizar únicamente software original legalmente adquirido y autorizado e instalado por el departamento de sistemas.
  - No debe instalar en la computadora software "pirata" ni de "juegos".

- No debe instalar "vacunas" sin la autorización de sistemas. Estas aunque parezca irónico, pueden estar infectadas.
- Estar atentos a los mensajes de alerta emitidos por el computador. El departamento de sistemas aplicará el detector de virus periódicamente.

ART. 8. SEGURIDAD FÍSICA DE LOS EQUIPOS Y DEL USUARIO:

- El solo contar con buenos programas de mantenimiento preventivo de los equipos de computación, no garantizan totalmente su operación satisfactoria, ni eliminan los riesgos de desperfecto que como cualquier elemento electrónico puede presentar. Pero si este equipo cuenta además con los cuidados de instalación, limpieza, temperatura, humedad, eléctricos, se estará brindando un estado óptimo de trabajo con un mínimo de revisiones y reparaciones.
- Las siguientes recomendaciones, acogidas por los usuarios de computadores, prolongarán la vida de los equipos:
  - Ubique el equipo en un área donde no exista mucho movimiento de personal.
  - No traslade la computadora sin la autorización y asesoría del departamento de sistemas.
  - Instale el computador sobre escritorios o muebles estables o especialmente diseñados para ello.
  - Ubique el equipo lejos de la luz del sol y de ventanas abiertas.
  - La energía eléctrica debe ser regulada a 110 voltios y con polo a tierra. Asesórese debidamente para garantizar una buena toma eléctrica
  - No conecte otros aparatos (Radios, máquinas de escribir, calculadoras, etc.) en la misma toma del computador.
  - Cada usuario, al momento de terminar las labores diarias, deberá apagar los equipos (Computadora , Impresoras, Escáneres),
  - Evite colocar encima o cerca de la computadora ganchos, clips, bebidas y comidas que se pueden caer accidentalmente dentro del equipo.
  - No fume cerca del equipo, el alquitrán se adhiere a las piezas y circuitos internos del equipo.
  - Mantenga libre de polvo las partes externas del computador y de las impresoras. Utilice un paño suave y seco. Jamás use agua y jabón. Solicite al técnico de mantenimiento una tarea total de limpieza de estos equipos.
  - Mantenga la pantalla y el teclado cubiertos con fundas plásticas cuando no haga uso de ellos por el tiempo considerable o si planea el aseo o reparaciones de las áreas aledañas al computador.
  - Utilice en la impresora el ancho del papel adecuado. El contacto directo de la cabeza de impresión sobre el rodillo puede estropear ambas parte. (Usuarios con impresoras de matriz de punto)
  - Está prohibido destapar y tratar de arreglar los equipos por su cuenta. En todos los casos asesórese del departamento de sistemas o del encargado de esta operación.
  - No preste los equipos o asegúrese que la persona que lo utilizará conoce su correcta operación.
  - Todas las pantallas de los equipos deberán contar con filtros antirreflectivos, los cuales deben ser solicitados por cada usuario.

La Dirección de Recursos Humanos en conjunto con la Dirección de Desarrollo Organizacional, la Unidad de Sistemas, deberá analizar, corregir y/o modificar la presente normativa institucional.

DISPOSICIONES GENERALES:

Art. 1.- Derogase en forma expresa cualquier normativa o disposición administrativa que se oponga total o parcialmente a la presente Resolución.
Art. 2.- Apliquese en forma obligatoria en toda la Institución, y en general a todos y todas las servidores públicos que laboran en el INAMHI, sin excepción alguna.
Art. 3.- De la aplicación y ejecución de la presente Resolución, encárguese a las Direcciones de Desarrollo Organizacional, con su Unidad de Informática y TICs; Dirección de Planificación; Dirección de Recursos Humanos o Talento Humano del Instituto Nacional de Meteorología e Hidrología.
Art. 4.- La presente Resolución entrará en vigencia desde la fecha de expedición legal, sin perjuicio de su publicación en el Registro Oficial.

COMUNÍQUESE Y CÚMPLASE

Dado, en la Dirección Ejecutiva del Instituto Nacional de Meteorología e Hidrología, en la ciudad de Quito, Distrito Metropolitano, a los treinta y un días del mes de marzo de dos mil catorce.

Carlos Hugo Naranjo Jácome
DIRECTOR EJECUTIVO DEL INAMHI

DIRECCIÓN DE ASESORÍA JURÍDICA
INAMHI
INSTITUTO NACIONAL DE METEOROLOGÍA E HIDROLOGÍA