FIRMAS DE APROBACIÓN

ELABORA:

Lic. Rafael Pimentel Pinto

Director de Gestión de la Información en Materia Espacial.

REVISA:

Lic. Tiburcio Montalvo Naranjo.

Coordinador General de Financiamiento y Gestión de la Información en Materia Espacial.

AUTORIZA:

Dr. Francisco Javier Mendieta Jiménez.

Director General.

1. INTRODUCCIÓN.

Corresponde a la Coordinación General de Financiamiento y Gestión de la Información en Materia Espacial emitir, en el ámbito de su competencia, la normatividad necesaria para el cumplimiento de sus funciones, y a la Dirección de Gestión de la Información en Materia Espacial, proponer las políticas y los lineamientos en materia de la gestión de la información espacial, para asegurar su consulta, guardando su integridad, disponibilidad y confidencialidad; de conformidad con lo establecido en el artículo 28 del Estatuto Orgánico de la Agencia Espacial Mexicana, publicado en el DOF el 27 de noviembre de 2012 y reformado el 10 de abril de 2015, y en el inciso a) del numeral 3.5.2 del Manual de Organización de la Agencia Espacial Mexicana, del 5 de diciembre de 2013, respectivamente, por lo que se han elaborado las presentes **Políticas para el uso de bienes y servicios informáticos (Políticas)**.

La base para que la Agencia Espacial Mexicana (AEM) opere de forma confiable y segura con los bienes y servicios informáticos, comienza con la definición de Políticas y estándares adecuados.

Las presentes Políticas se revisarán anualmente en la 1ra sesión ordinaria del Grupo de Trabajo de Dirección de Tecnologías de Información y Comunicaciones (GTDTIC) con el objeto de mantenerlas actualizadas, por parte de los responsables de su elaboración.

2. OBJETIVO.

Dar a conocer las Políticas, que debe observar y cumplir el personal de la AEM, a efecto de proteger adecuadamente la información propiedad de la Institución y los activos tecnológicos, así como aprovechar de la mejor manera los servicios informáticos que son compartidos entre todas las áreas.

3. CRITERIOS DE OPERACIÓN.

I. El incumplimiento a las presentes Políticas, podrá presumirse como causa de responsabilidad administrativa y/o penal, dependiendo de su naturaleza y gravedad, cuya sanción será aplicada por las autoridades competentes.

II. Las Políticas deben ser cumplidas de manera obligatoria por el personal de la AEM, para el buen uso de los bienes y servicios informáticos, y son la base para la protección de la información institucional. Asimismo, su incumplimiento puede conducir a condiciones de operación crítica, inestabilidad, intermitencias y alteraciones de afectación general.

III. El personal de la AEM, tiene la responsabilidad de usar los bienes y servicios informáticos, exclusivamente con propósitos directamente relacionados con sus funciones, y de una manera ética, profesional y apegada a la normatividad vigente, sin olvidar la prioridad, importancia y el valor que tiene la información para la Institución.

IV. Todas las actividades que realice el personal de la AEM, en los bienes y servicios informáticos, son susceptibles de auditoría.

V. Se considera una falta grave, la instalación de cualquier tipo de software en los bienes informáticos de la AEM, que no hayan sido autorizados por el titular de la Dirección de Gestión de la Información en Materia Espacial.

VI. Los sistemas (software) adquirido por la AEM, o desarrollado por personal, interno o externo, que sea parte de la AEM o sea coordinado por ésta, son propiedad intelectual de la misma y está prohibido por las leyes de derechos de autor y por la AEM, realizar copias no autorizadas de dicho software.

VII. Se considera una falta grave y un ataque a la seguridad informática, cualquier actividad no autorizada, de exploración de los recursos informáticos en la red de la AEM, para violar o intentar violar los mecanismos de seguridad como el antivirus, firewall, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y mostrar una posible vulnerabilidad.

VIII. Los mensajes del correo electrónico institucional y archivos adjuntos, son información propiedad de la AEM y deben ser manejados como una comunicación privada y directa entre emisor y receptor.

IX. El Director General podrá solicitar el acceso y revelar todos los mensajes enviados a través del correo electrónico institucional.

X. Los recursos informáticos no son ilimitados, por lo que el nivel máximo para envío y recepción del correo electrónico será de 25 MB. El ancho de banda de la red y la capacidad de almacenamiento tienen límites, y todo el personal de la AEM conectado a la red tiene la responsabilidad de conservar estos recursos, por lo que no debe realizar deliberadamente actos que los desperdicien ni los monopolice. **Se deberá utilizar la firma institucional, así como la leyenda que la DGIME indique.**

XI. Las cuentas de correo electrónico del personal de la AEM, que cause baja de la Institución, serán configuradas para redireccionarlas a los correos del personal que lo reemplaza y, en

caso de que no existiera, al superior jerárquico que corresponda, por un periodo de 15 días naturales, a partir de la fecha de su baja.

XII. Se consideran usos inadecuados del correo electrónico:

1) El uso de palabras, imágenes o referencias que puedan ser vistas como difamatorias, hostiles, ilegales, discriminatorias u ofensivas o de índole político.

2) Generar o transmitir información de cualquier tipo que pueda ser considerada inapropiada, de manera enunciativa mas no limitativa, obscena o pornográfica, hostil u ofensiva referente a raza, sexo, edad, preferencia sexual, estado civil, religión, nacionalidad y/o discapacidad.

3) Descargar, copiar o transmitir información protegida por derechos de autor en violación de estos derechos, con el conocimiento y/o anuencia del usuario.

4) El uso de dispositivos de codificación (encriptación) no autorizados.

5) La transmisión no autorizada de mensajes a múltiples usuarios.

6) Cualquier mensaje que por su estructura o contenido sea considerado como SPAM (cadenas de mensajes con fines personales, mensajes grupales no institucionales, mensajes comerciales no solicitado o subversivos enviados a un grupo, propaganda política, etc.)

7) La difusión de información considerada como reservada o confidencial, en los términos de la Ley Federal de Transparencia y Accesos a la Información Pública Gubernamental.

8) Cualquier otro uso que no apoye el desempeño de las funciones propias del personal de la AEM.

XIII. Se considera falta grave escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para auto replicarse, dañar o en otros casos impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema o software. Así como probarlos en cualquiera de los ambientes o plataformas de la AEM.

XIV. El acceso a internet provisto al personal de la AEM, es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña. En caso de daño a la imagen de la institución se procederá de acuerdo a lo que determine el Órgano Interno de Control.

XV. El Director de Gestión de la Información en Materia Espacial podrá instruir bloquear el acceso a sitios de Internet con contenido ajeno a las funciones de las diversas áreas y a establecer el esquema de filtrado de contenidos según su categoría.

XVI. El personal de la AEM, es responsable de su identificador de usuario y contraseña, necesarios para acceder a la información y a los bienes y servicios informáticos, por lo cual debe mantenerlo de forma confidencial, y el mal uso de ellos será responsabilidad del servidor público que lo proporcionó.

XVII. El Director General podrá solicitar la implementación de mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los bienes y servicios informáticos que sea detectado, será reportado conforme a lo indicado en estas políticas.

4. RESPONSABILIDADES.

I. El titular de la Coordinación General de Financiamiento y Gestión de la Información en Materia Espacial, es el facultado para definir Políticas en materia de uso de bienes y servicios informáticos que se otorgan al personal de la AEM.

II. Todo el personal de la AEM es responsable de cumplir, obligatoriamente, estas Políticas.

III. El titular de la Dirección General y los titulares de las Coordinaciones Generales, de las Direcciones de área y Gerencias, son responsables de la supervisión del cumplimiento de las Políticas.

IV. La Dirección de Administración es responsable de hacerlas del conocimiento a los empleados de nuevo ingreso, a efecto de que se lleve a cabo su debido cumplimiento.

V. Todos los servidores públicos de la AEM, son responsables de remitir el reporte o denuncia correspondiente al titular del Órgano Interno de Control de la AEM, para los efectos de su competencia y atribuciones, en caso de que detecten el incumplimiento de las Políticas.

VI. El titular de la Dirección General y los titulares de las Coordinaciones Generales, son responsables de solicitar al titular de la Coordinación General de Financiamiento y Gestión de la Información en Materia Espacial, la asignación de bienes y servicios informáticos para el personal de la AEM.

VII. El titular de la Coordinación General de Financiamiento y Gestión de la Información en Materia Espacial es quien autoriza la asignación de bienes y servicios informáticos al personal de la AEM, con base en la justificación clara y concisa de la necesidad real, así como en los criterios normativos y disponibilidad presupuestaria.

VIII. El titular de la Dirección de Gestión de la Información en Materia Espacial, es responsable de administrar y proveer al personal de la AEM, los bienes y servicios informáticos, autorizados.

IX. El titular de la Gerencia de Recursos Financieros y Materiales, es responsable de que toda persona, incluyendo al personal de la AEM, registre los bienes informáticos de su propiedad, al ingresar a las oficinas de la AEM.

5. POLÍTICAS RELACIONADAS CON LOS BIENES Y SERVICIOS INFORMÁTICOS.

I. El personal de la AEM, a quien se le asigne bienes informáticos, se obliga a:

1) Firmar el documento de asignación o resguardo correspondiente, y a partir de ese momento ser responsable de su custodia y buen uso.

2) No prestarlos, ya que su asignación o resguardo, tiene el carácter personal y es intransferible.

3) Almacenar información que genere y obtenga durante el desempeño de sus funciones y deba ser respaldada, únicamente en la unidad de red denominada "AEMdocs". La DGIME no será responsable de la información que no se encuentre en este directorio.

4) Evitar en todo momento la fuga de la información de la AEM, contenida en los bienes informáticos que tiene asignados o bajo su resguardo.

5) Protegerlos, aún y cuando no los utilice, y contengan o no información reservada o confidencial.

6) Reportar de forma inmediata, al personal de la Dirección de Gestión de la Información en Materia Espacial, los riesgos reales o potenciales como pueden ser fugas de agua, conatos de incendio u otros.

7) No consumir alimentos o ingerir líquidos, mientras los opera.

8) Evitar colocar objetos encima de ellos y a no cubrir los orificios de ventilación.

9) Mantener un entorno limpio alrededor de ellos.

10) Asegurarse que los cables de conexión no sean pisados o aplastados al colocar otros objetos encima o contra ellos.

11) No abrirlos o desarmarlos.

12) No reubicarlos, instalarlos o desinstalarlos, ni retirar sellos de los mismos; en caso de requerir este servicio, deberá solicitarlo al personal de la Dirección de Gestión de la Información en Materia Espacial.

13) Solicitar la identificación del personal autorizado para llevar a cabo la asignación de los bienes y servicios informáticos, así como su reparación, antes de permitir el acceso a sus equipos o el retiro de los mismos.

14) Apagarlos en su totalidad al final de la jornada laboral.

15) Solicitar a su superior jerárquico la capacitación para el manejo de las herramientas informáticas que utiliza, a fin de evitar riesgos por mal uso y para aprovecharlas al máximo.

16) Cubrir el valor de la reparación o reposición, en caso de que se determine que alguna descompostura, se originó por maltrato, descuido o negligencia.

17) En caso de que haya sufrido el robo de algún bien informático, realizar las gestiones ante la autoridad judicial o jurisdiccional correspondiente, y dar aviso de inmediato al personal de la Dirección de Gestión de la Información en Materia Espacial.

II. El personal de la Dirección de Gestión de la Información en Materia Espacial, se obliga a:

1) Asegurar que sólo el personal autorizado pueda acceder a los Centros de Datos de la AEM, considerados como áreas restringidas.

2) Autorizar al personal que debe llevar a cabo la asignación de los bienes y servicios informáticos a todo el personal de la AEM, así como su reparación.

3) Asegurar que, el personal autorizado para llevar a cabo la asignación, servicios, reparación o baja de bienes informáticos durante su estancia en la AEM, esté debidamente identificado.

4) Asesorar al personal de la AEM para que realice el respaldo de los archivos contenidos en el disco duro u otra unidad de almacenamiento del equipo que presente alguna falla y sea enviado a reparación, previniendo así la pérdida involuntaria de información.

5) Asesorar al personal de la AEM para que, la información sensible que se encuentre en el equipo que presente alguna falla y sea enviado a reparación, sea borrada, una vez realizado el respaldo de la misma.

6. POLÍTICAS RELACIONADAS CON LA OPERACIÓN.

I. El personal de la AEM, quien utilice bienes y servicios informáticos, se obliga a:

1) Utilizar los mecanismos institucionales para proteger la información que reside y utiliza en los bienes informáticos.

2) Bloquear los equipos cuando se levanten de sus lugares.

3) Proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna o hacia redes externas como internet.

4) En el caso de requerir un medio compartido de almacenamiento de información en red, el responsable de la información a compartir, deberá solicitarlo a la DGIME. Indicando a quiénes será compartido y los permisos que serán asignados (lectura, escritura o control total).

5) En caso de ser necesario, otorgar acceso únicamente a la red inalámbrica denominada "INVITADOS", a las personas ajenas a la Institución y que por motivos de trabajo se encuentren en las instalaciones de la AEM.

6) Respaldar de manera diaria, en la unidad de red denominada "AEMdocs", toda la información Institucional con la que cuente, a efecto de que se realicen los respaldos diarios de toda la Institución y evitar la pérdida de información.

7) Conservar la contraseña de encripción, de la información sensible y crítica que haya cifrado con la herramienta que la Dirección de Gestión de la Información en Materia Espacial le proporcione para tal fin, pues en caso de olvidarla no será posible recuperar la información.

8) Conservar los registros o información que se encuentra activa y aquélla que ha sido clasificada como reservada o confidencial, de conformidad a las disposiciones en materia de transparencia y acceso a la información.

9) No instalar software adicional al existente en la imagen base de los bienes informáticos. En caso de requerirlo, solicitar a la DGIME y presentar la justificación, para su autorización. En caso de contar con la licencia del software se deberá presentar la factura de compra o certificado de licenciamiento.

10) Notificar a su jefe inmediato, cuando tenga la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada.

11) Reportar al personal de la DGIME, a través del medio que se indique, cualquier incidente generado durante la operación de los bienes y servicios informáticos.

12) No establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la AEM. En caso de requerirlo presentar la justificación a la DGIME, para su autorización.

13) No instalar herramientas de seguridad como antivirus, firewalls, proxys u otros mecanismos de seguridad.

14) Utilizar el correo electrónico institucional, en forma profesional, cortés y en cumplimiento de las políticas y leyes aplicables.

15) No usar cuentas de correo electrónico institucional asignadas a otras personas, ni recibir mensajes en cuentas de otros servidores públicos. En caso de requerir la delegación de buzón o calendario, solicitarlo a la DGIME.

16) No redireccionar los correos institucionales a una dirección de correo electrónico externa comercial o personal, a menos que cuente con la autorización del titular de la Dirección General de la AEM.

17) Enviar a través del correo electrónico institucional, información reservada y/o confidencial exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones.

18) Utilizar el correo electrónico institucional, única y exclusivamente para los recursos que tenga asignados y las facultades que les hayan sido atribuidas para el desempeño de su empleo, cargo o comisión, quedando prohibido cualquier otro uso distinto.

19) No falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico institucional.

20) Evitar hacer uso de cualquier clase de software que no haya sido proporcionado o autorizado por la DGIME.

21) No descargar y/o almacenar en los bienes informáticos o transmitir a través de ellos, videos, música, gráficos o ejecutables no relacionados con la actividad propia de la AEM, que provengan de internet, correo electrónico, y cualquier dispositivo de almacenamiento por ejemplo USB o en CD.

22) No extraer información de los bienes informáticos a través de cualquier dispositivo de almacenamiento por ejemplo USB o en CD.

23) Dejar de usar inmediatamente el equipo y llamar a la Dirección de Gestión de la Información en Materia Espacial, en caso de detección o sospecha de alguna infección por virus de computadora, el cual debe erradicarse inmediatamente.

24) No alterar o eliminar las configuraciones de seguridad para detectar y/o prevenir la propagación de virus en los bienes informáticos, tales como:

- Antivirus;
- Correo electrónico;
- Paquetería Office;
- Navegadores; u
- Otros programas.

25) En caso de requerir un acceso a internet fuera de la red institucional deberá utilizarse la red privada virtual (VPN) utilizada por la DGIME.

26) Permitir el monitoreo de las actividades que realizan en internet.

27) No acceder a páginas web o sitios web, no autorizados.

28) No utilizar el servicio de internet para propósitos personales, como para difundir, visualizar o almacenar anuncios personales o comerciales, ofertas de servicios, promociones, códigos destructivos (por ejemplo, programas conocidos como virus, troyanos, etc.) o cualquier otro material que ponga en riesgo la seguridad e información de la AEM o acceder a juegos en Internet, participar en charlas en línea o redes sociales si esto no está directamente relacionado con las funciones propias del área.

29) Los bienes informáticos personales (celulares, smartphone, laptops, tablet, etc.) solo podrán acceder a internet mediante la red BYOD AEM, previa solicitud a la DGIME.

30) No utilizar en las cuentas institucionales la misma contraseña, que utiliza para sitios seguros como bancos y en servicios gratuitos de correo.

II. El personal de la Dirección de Gestión de la Información en Materia Espacial, se obliga a:

1) Proporcionar una cuenta de correo electrónico institucional al personal de la AEM, para el cumplimiento de sus funciones y actividades que desempeñan para la Institución.

2) Proporcionar al personal de la AEM las herramientas para encriptar información.

3) Atender inmediatamente reportes de virus, en caso de detección o sospecha de alguna infección.

7. POLÍTICAS RELACIONADAS CON LOS CONTROLES DE ACCESO LÓGICO.

I. El personal de la AEM, quien utilice bienes y servicios informáticos, se obliga a:

1) Responsabilizarse de su identificador de usuario y contraseña, para el uso y acceso a los bienes y servicios informáticos.

2) Autenticarse por los mecanismos de control de acceso, para el uso y acceso a los bienes y servicios informáticos.

3) No proporcionar información a personal externo, de los mecanismos de control de acceso a los bienes y servicios informáticos.

4) No compartir su identificador de usuario y contraseña, ya que todo lo que ocurra con ese identificador y contraseña será responsabilidad exclusiva del usuario al que pertenezcan.

5) No usar el identificador de usuario y contraseña de otros, aunque ellos les insistan en usarlo.

6) Notificar a la Dirección de Gestión de la Información en Materia Espacial, cualquier cambio en los roles y responsabilidades del personal de la AEM que modifique sus privilegios de acceso a los bienes y servicios informáticos.

7) Reportar a la DGIME, cuando olvide, bloquee o extravíe su contraseña.

8) No tener los identificadores de usuarios y contraseñas en forma visible, en cualquier medio impreso o escrito en el área de trabajo, de manera de que se permita a personas no autorizadas su conocimiento.

9) Observar los siguientes lineamientos para la construcción de sus contraseñas:

- No deben contener números consecutivos;
- Deben estar compuestos de al menos seis (6) caracteres y máximo diez (10). Estos caracteres deben ser alfanuméricos.
- Deben ser difíciles de adivinar, esto implica que las contraseñas no deben relacionarse con el trabajo o la vida personal del usuario.
- Deben ser diferentes a las contraseñas que se hayan usado previamente.

10) Cambiar inmediatamente su contraseña cuando tenga la sospecha de que es conocida por otra persona.