Reglas internas para uso de los Activos de Tecnologías de la Información, Comunicaciones y Seguridad de la Información en el Instituto Nacional de Medicina Genómica.

Marzo 2026

Índice

CONSIDERANDOS

Que de acuerdo a lo establecido en el artículo 7 bis, fracción V de la Ley de los Institutos Nacionales de Salud, el INMEGEN tendrá la atribución de fomentar la realización de proyectos de desarrollo de tecnología especializada, obteniendo con ello protocolos de innovación tecnológica en cuanto a la elaboración de medios de diagnóstico.

Que el artículo 20 fracción IX de la Ley General de Transparencia y Acceso a la Información Pública, establece que el INMEGEN como sujeto obligado deberá fomentar el uso de tecnologías de la información para garantizar la transparencia, el ejercicio del derecho de acceso a la información y la accesibilidad a éstos.

Que el Estatuto Orgánico del Inmegen, en el artículo 33, fracción XVII, la Dirección de Administración tiene la facultad de definir, establecer y difundir las políticas y procedimientos en materia de Tecnologías de la Información, y de la Comunicación, en apego a la normatividad y estándares nacionales e internacionales aplicables; en la fracción XVIII, procurar la asistencia técnica y continuidad a la infraestructura de tecnología de la información, comunicación y seguridad de la información y en la fracción XIX, proveer los servicios necesarios en materia de tecnologías de la información, comunicación y seguridad de la información, así como todas aquellas funciones establecidas por el Gobierno Digital, para el desarrollo de las actividades del Instituto.

Conforme al ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal publicado el 6 de septiembre de 2021 y a la reforma a la Ley Orgánica de la Administración Pública Federal, publicada en el Diario Oficial de la Federación el 28 de noviembre de 2024, se cuenta con el programa Sectorial 2025-2030 emitido por la Agencia de Transformación Digital y Telecomunicaciones.

Que en lo que precisa la Ley Federal de Austeridad Republicana, artículo 16 fracción III, se prioriza el uso de software libre en las adquisiciones, arrendamientos de equipos y sistemas de cómputo, siempre que este cumpla con las características requeridas para el ejercicio de las funciones públicas.

Que del ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal, en su capítulo II, establece las políticas tecnológicas generales.

Que el uso de las Reglas internas para uso de los Activos de Tecnologías de la Información, Comunicaciones y Seguridad de la Información en el Instituto Nacional de Medicina

Genómica es de suma importancia, debido a que de esta manera se regula, gestiona y administra toda la infraestructura tecnológica identificada como propiedad del INMEGEN y la integración de nuevas herramientas tecnológicas. (hardware, software, navegación en internet, correo electrónico institucional, telefonía, respaldos de información, desarrollo de software y seguridad de la Información) para ser aprovechados de la mejor forma para desempeñar las labores sustantivas y operativas maximizando la interoperabilidad de los activos de tecnologías de la Información.

Que es importante tomar las medidas pertinentes, ya que son herramientas tecnológicas de trabajo que necesita el personal del INMEGEN para el desempeño de sus labores diarias. El apego a estas indicaciones permite salvaguardar la seguridad de la información que se genera diariamente dentro del instituto. Estas reglas internas disminuyen el riesgo de vulneración y que los recursos con los que se cuentan, sean utilizados únicamente con fines laborales, lo que impactará de manera positiva en el logro de los objetivos institucionales.

Es importante mencionar que las reglas internas para uso de los Activos de Tecnologías de la Información, Comunicaciones y Seguridad de la Información en el Instituto Nacional de Medicina Genómica coadyuvan y no se sobreponen a ninguna disposición, acuerdo, reglamento y/o Ley oficial sobre la materia.

Capítulo I

Generalidades.

Artículo 1.- Las presentes reglas internas tienen por objeto establecer un marco claro de control para el aprovechamiento y uso óptimo de los activos de Tecnologías de la Información, Comunicaciones y Seguridad de la Información , salvaguardando la confidencialidad, integridad y disponibilidad de la información contenida en las bases de datos, aplicativos y sistemas que provee el Instituto Nacional de Medicina Genómica o que sus colaboradores generan, con la finalidad de crear una cultura de seguridad de la información, control y uso de las tecnologías de la información y comunicación.

Artículo 2.- Para los efectos de estas reglas internas se entenderá por[1]**:**

I. **Acuerdo de Confidencialidad:** Instrumento que se celebra entre las partes para restringir el uso o divulgación pública o hacia terceros de la información o conocimiento que se trate con motivo de la relación existente.

[1] https://www.ift.org.mx/comunicacion-y-medios/glosario-de-terminos
ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal. Publicado en DOF el 6 de septiembre de 2021.

II. **Activo de información:** la información, los datos y los recursos que la contienen, procesan y transmiten, que por su importancia y el valor que representa para una Institución, deben ser protegidos.

III. **Activo de información esencial:** el activo de información cuya destrucción, pérdida, alteración o falla tendría un grave impacto o consecuencia en la funcionalidad de la infraestructura de TIC o en los servicios que soporta.

IV. **Activo Tecnológico:** hardware, sistemas de software o información que tienen valor para una organización.

V. **Amenaza:** el posible acto o circunstancia interna o externa que puede explotar, de manera intencional o circunstancial, la debilidad presente en un activo de información. Una amenaza puede tener diferente nivel de riesgo de acuerdo con los escenarios en los que se presente.

VI. **Archivo:** conjunto de datos o instrucciones que se almacenan en el disco duro y/o cualquier otro medio de almacenamiento con un nombre que los identifica.

VII. **Arquitectura Institucional:** el enfoque mediante el cual se estructuran los componentes de la Institución (procesos, información, arquitectura tecnológica y personas) delineando sus relaciones y evolución en el tiempo, permite a las áreas de TIC entender y atender sus necesidades desde una perspectiva integral y estratégica, aportando valor.

VIII. **Arquitectura tecnológica:** la estructura de hardware, software y redes de telecomunicación requerida para dar soporte a la implementación de los aplicativos de cómputo, soluciones tecnológicas o servicios de TIC en la Institución.

IX. **Autorización:** permiso para efectuar acciones sobre elementos del sistema de información otorgado a un Usuario.

X. **Biblioteca Única de Software:** base de datos de las Licencias de Software que son propiedad o están a cargo del INMEGEN.

XI. **Borrado Seguro:** El borrado seguro es la medida de seguridad mediante la cual se establecen métodos y técnicas para la eliminación definitiva de los datos, de modo que la probabilidad de recuperarlos sea mínima

XII. **Confidencialidad:** garantizar que la información no sea accesible por personas no autorizadas.

XIII. **Contraseña:** clave para obtener acceso a un programa o partes de un programa determinado, una terminal u ordenador personal (computadora portátil o de escritorio), un punto en la red (fijo o inalámbrico), etcétera.

XIV. **Correo electrónico institucional:** servicio de comunicación y transmisión de mensajes en línea, a través de una computadora u otro dispositivo electrónico a través de redes informáticas, que constituye una herramienta de trabajo, para el desempeño de las facultades, competencias o funciones de los usuarios y unidades administrativas del INMEGEN a través de los dominios institucionales (@inmegen.gob.mx, @inmegen.edu.mx o @inmegen.org).

XV. **Control de seguridad de la información:** las medidas establecidas para preservar la confidencialidad, integridad y disponibilidad de la información Institucional contra las amenazas latentes o existentes y, que coadyuvan en la gestión de riesgos inherentes a su uso.

XVI. **Disponibilidad:** garantizar que la información esté accesible cuando se necesite.

XVII. **Dueño de la Información:** Es el personal Directivo que puede tomar una decisión del uso o finalidad de la Información de dicha área independientemente del activo de información.

XVIII. **Endpoint:** cualquier dispositivo que está conectado a una red informática (Equipo de cómputo, Switch de datos, switch inalámbrico, equipo telefónico, router, modem, servidor, etc.).

XIX. **Equipo de cómputo:** son los dispositivos eléctricos, electrónicos y mecánicos que se emplean para procesar o consultar, transmitir, almacenar datos.

XX. **Hardware:** el conjunto de componentes físicos electrónicos que procesan y/o transmiten datos y que forman parte de la Infraestructura Tecnológica del Inmegen.

XXI. **Incidente:** Acontecimiento, ocurrencia y/o situación que, al presentarse, pueda llevar a una interrupción de los servicios.

XXII. **INMEGEN:** Instituto Nacional de Medicina Genómica.

XXIII. **Información:** datos que tienen un significado en algún contexto para su receptor.

XXIV. **Integridad:** La exactitud, consistencia y conservación de la información sin ninguna alteración no autorizada.

XXV. **Internet:** servicio de red informática que provee conectividad de los Usuarios del Inmegen con el resto del mundo, como herramienta de trabajo para el ejercicio de la función encomendada.

XXVI. **Interoperabilidad:** la capacidad de organizaciones y sistemas dispares y diversos, para interactuar con objetivos consensuados y comunes con la finalidad de obtener beneficios mutuos, en donde la interacción implica que las Instituciones compartan infraestructura, información y conocimiento mediante el intercambio de datos entre sus respectivos sistemas de tecnología de información y comunicación.

XXVII. **Licencia:** permiso legal otorgado por un tercero con facultades para ello, para utilizar un producto, generalmente Software, a cambio de un pago único o periódico.

XXVIII. **Mantenimiento Correctivo:** la reparación de equipos que presentan alguna falla en su operación.

XXIX. **Mantenimiento Preventivo:** revisión y reacondicionamiento de los activos de Tecnologías de la Información y comunicación en forma programada, para prevenir fallas en la operación de los mismos.

XXX. **Malware**: software malicioso o indeseado diseñado para infiltrarse en los endpoint sin consentimiento.

XXXI. **Mesa de Ayuda de Tecnologías de la Información:** sistema de contacto para la recepción, administración y gestión de incidentes de tecnologías de la Información.

XXXII. **Navegador de Internet:** Aplicación de Software que permite al usuario, visualizar e interactuar con servidores web de todo el mundo a través de la red.

XXXIII. **Periféricos:** accesorio electrónico de entrada y/o salida de información, que pueden ser conectados a un Equipo de Cómputo.

XXXIV. **Persona Servidora Pública:** es la persona que desempeña un empleo, cargo o comisión subordinada al Estado.

XXXV. **Red LAN:** Interconexión física o inalámbrica de área local que interconecta uno o más dispositivos, en un mismo edificio.

XXXVI. **Red WLAN**: Red inalámbrica de área local que emplea ondas de radio para proveer conectividad entre uno o más dispositivos en un mismo edificio.

XXXVII. **Riesgo:** la probabilidad de que una amenaza pueda explotar una vulnerabilidad, generando un impacto sobre la infraestructura de TIC y los Activos de Tecnologías de la Información.

XXXVIII. **Seguridad de la Información:** capacidad de preservar la confidencialidad, Integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma.

XXXIX. **Servicios en la Nube:** al modelo de provisión externa de servicios de cómputo bajo demanda que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente, que se encuentren localizados fuera o dentro del territorio nacional, en instalaciones del Estado o en instalaciones privadas

XL. **Servidor:** Endpoint, hardware o software que proporciona a otros activos de tecnologías de la Información y comunicación en la misma red, acceso a información, programas, servicios o espacio de almacenamiento.

XLI. **Software:** conjunto de sistemas operacionales, programas, productos y aplicaciones que utiliza el Inmegen.

XLII. **Software libre:** el programa informático cuyo código fuente cumple con las cuatro libertades del Software Libre y por ende se encuentra disponible para ser ejecutado, estudiado, modificado o distribuido libremente, independientemente de su costo o gratuidad.

XLIII. **Shareware:** tipo de Software que se distribuye gratuitamente y que tiene limitaciones de uso con respecto a una versión completa.

XLIV. **Tecnologías de la información y comunicación**: el equipo de cómputo, software, dispositivos de impresión, infraestructura y servicios que sean utilizados para almacenar, procesar, convertir, proteger, transferir, y recuperar información, datos, voz, imágenes y vídeo.

XLV. **Usuario final:** persona servidora pública, estudiantes y de servicio social del INMEGEN que hace uso de los activos de tecnologías de la información y comunicación que son propiedad del Instituto.

XLVI. **Vulnerabilidad:** debilidad de un activo tecnológico o control de seguridad que pueda ser explotado por una o más amenazas.

Artículo 3.- Las presentes reglas internas son de carácter obligatorio y aplicables a cualquier usuario fiinal o usuario final que sea autorizado para el uso de los activos de Tecnologías de la Información y Comunicación del INMEGEN.

Artículo 4.- Las personas servidoras públicas de la Dirección de Administración, en colaboración con la Subdirección de Tecnologías de la Información son responsables de verificar el cumplimiento de los presentes Reglas.

Artículo 5.- El uso de los activos de la Información y Comunicación es personal e intransferible y serán asignados para realizar funciones estrictamente institucionales únicamente a una persona servidora pública con una relación laboral de confianza o base.

Artículo 6.- En el caso de que algún usuario final requiera alguna precisión a estas Reglas, las personas servidoras públicas de la Dirección de Administración y de la Subdirección de Tecnologías de la Información atenderán cualquier solicitud puntual hecha por escrito.

Artículo 7.- La Subdirección de Tecnologías de la Información deberá asignar e instalar, únicamente el Software que cuente con Licencia de uso vigente y el Hardware que hayan sido adquiridos, arrendados o donados al Inmegen.

Capítulo II

Reglas internas específicas.

Artículo 8.- Con el propósito de mantener los activos de Tecnológias de la Información y Comunicación propiedad del Instituto en condiciones adecuadas para su uso, es responsabilidad de cada usuario final resguardante adoptar las siguientes medidas:

I. Cumplir con la normatividad vigente en materia de responsabilidades aplicables a las Personas servidoras públicas del Instituto.

II. Evitar deshabilitar los mecanismos de seguridad que se encuentran configurados en los equipos de cómputo y portátiles del instituto, tales como antivirus, antimalware, firewall, etcétera.

III. No tomar líquidos ni colocar objetos o alimentos sobre ni junto a los activos de tecnologías de la información y comunicación y sus periféricos, así como dispositivos de entrada y/o salida.

IV. No dejar caer objetos sobre los equipos de cómputo y/o periféricos, tales como grapas, clips o cualquier otro elemento.

V. Apagar los activos de tecnologías de información y comunicación cuando no se encuentre en uso y obligatoriamente al finalizar la jornada laboral.

VI. Cerrar las aplicaciones o programas de Software que no estén en uso.

VII. Reportar a través de los canales dispuestos de la Mesa de Ayuda de Tecnologías de la Información, cualquier incidente y/o solicitud relacionada con la Arquitectura de Tecnologías de la Información, Comunicación y Seguridad de la Información del INMEGEN.

VIII. Como usuario responsable y/o dueño de los activos de información asignados, que maneja, recibe, transmite y/o genera información, deberá depurar de forma periódica el correo electrónico, equipo de cómputo y demás activos que le sean asignados, a fin de no sobrepasar el almacenamiento.

IX. Es responsabilidad del usuario final salvaguardar la información de los activos de Tecnologías de la Información y Comunicación.

X. Evitar instalar cualquier software que no esté avalado por la Subdirección de Tecnologías de la Información, para lo cual deberá levantar un ticket para su atención, la cual estará en espera del VoBo de la Subdirección de Tecnologías de la Información.

XI. Bloquear el equipo de cómputo cuando se ausente de su lugar, evitando accesos no autorizados o uso del correo Institucional al dejar la sesión abierta

Artículo 9.- El uso de los activos de Tecnologías de la Información y comunicación por parte del usuario final es único y exclusivo para el desempeño de sus actividades institucionales encomendadas, por lo que tienen prohibido lo siguiente:

I. Manipular de los controles de seguridad que posea el activo de tecnologías de la información y comunicación, ya que puede propiciar la falla, daño o pérdida de activos tecnológicos y de información.

II. Cambiar la configuración física y/o lógica de cualquier activo de tecnologías de la información y comunicación;

III. Instalar, conectar y/o configurar, activos de Tecnologías de la Información y Comunicación a la Arquitectura Tecnológica del Instituto.

IV. Realizar acciones que afecten parcial o totalmente la operación de la Arquitectura Tecnológica y los activos de Tecnologías de la información y comunicación del Instituto.

V. Examinar o utilizar activos de tecnologías de la Información, de otro usuario final sin la previa autorización del resguardante o superior jerárquico.

VI. Instalar o ejecutar cualquier tipo de software que permite evadir las políticas de seguridad institucionales para el acceso a sitios web restringidos.

VII. Ayudar, promover u ocultar el uso no autorizado de servicios, sistemas, software o hardware ajenos al Instituto o para los que no se haya otorgado un permiso expreso de acceso.

VIII. Propiciar la vulneración de los activos de información y de Tecnologías de la Información y Comunicación.

Artículo 10.- Todo Usuario deberá utilizar los recursos relacionados con las Tecnologías de la Información y Comunicaciones del INMEGEN exclusivamente para el propósito por el cual le fueron asignados.

Artículo 11.- La información que se genera, resguarda y almacena es propiedad del INMEGEN, el usuario final a quién le sea asignado cualquier tipo de activo será responsable de salvaguardar su seguridad, integridad y disponibilidad, aunado a lo siguiente:

I. El respaldo de la Información contenida en los activos de Tecnologías de la Información y comunicación estará bajo su resguardo.

II. Hacer uso único y exclusivo de los Activos de Tecnologías de la Información y comunicación institucionales para el intercambio de información.

III. Implementar controles de seguridad para los Activos de Tecnologías de la Información que se compartan por medio de los activos de tecnologías de la información y comunicación o de manera física.

IV. Dar cabal cumplimiento al acuerdo de confidencialidad celebrado entre la persona servidora pública y el Inmegen.

V. No se recomienda para almacenamiento y transporte de información, el uso de dispositivos tales como smartphones o cualquier otro dispositivo móvil, toda vez que la confidencialidad, integridad y disponibilidad de la información del Inmegen puede ser vulnerada.

Artículo 12.- Es responsabilidad del usuario final considerar las siguientes directrices con respecto a la Arquitectura Tecnológica que le es asignado o a la que tuvieran acceso en el Inmegen, con el objeto de apoyar el óptimo desempeño de sus funciones:

I. Sobre uso de Hardware.

a) Cualquier activo de tecnologías de la información y comunicación propiedad del INMEGEN que no haya sido asignado a un usuario final, deberá ser registrado ante el área de activo fijo, y resguardado por la Subdirección de Tecnologías de la Información.

b) La Subdirección de Tecnologías de la Información almacenará todo activo de tecnologías de la Información y comunicación propiedad del INMEGEN en un área destinado para este propósito.

c) La asignación de activos de tecnologías de la Información y comunicación que existan en el almacén de la Subdirección de Tecnologías de la Información, será a través de un correo electrónico Institucional o ticket de servicio a la Mesa de Ayuda de Tecnologías de información por parte del jefe inmediato con nivel mínimo de Subdirección, en el cual adicionalmente incluirá: Nombre completo, cargo oficial, funciones principales y ubicación.

d) Es atribución de la Subdirección de Tecnologías de la Información, dictaminar la necesidad de hardware para el INMEGEN.

e) La Subdirección de Tecnologías de la Información dará a conocer por los medios oficiales el inicio de los mantenimientos preventivos a los Activos de Tecnologías de la Información, Comunicación y Seguridad de la Información propiedad del INMEGEN.

f) El activo de tecnologías de la Información y comunicación propiedad del INMEGEN que se requiera emplear fuera del Instituto, deberá ser notificado a la Mesa de Ayuda de Tecnologías de la Información para completar el formato destinado para este propósito.

g) En todo momento, el usuario final es responsable de la Integridad del activo de tecnologías de la Información y comunicación, software y hardware que sea entregado y/o asignado por parte del Subdirector de Tecnologías de la Información, quedando establecido en los formatos que se determinen para este propósito.

h) El equipo de cómputo científico, servidores, cómputo especializado y las unidades de almacenamiento de las que hagan uso, será regido por los instrumentos establecidos por las Subdirecciones de Secuenciación y Genotipificación y de Bioinformática en la normateca Institucional.

i) El uso de los dispositivos de impresión, digitalización y fotocopiado, deberá restringirse exclusivamente a asuntos de carácter oficial, utilizando en sustitución correos electrónicos, dispositivos de almacenamiento electrónico, digitalización en discos y todo tipo de medios electrónicos en apego a los LINEAMIENTOS en materia de Austeridad Republicana de la Administración Pública Federal.

j) La instalación y configuración de dispositivos de impresión, digitalización y fotocopiado se realizará para el usuario final de estructura o base con equipo de cómputo propiedad del Instituto.

II. Sobre uso de Software.

a) Cualquier licencia de software deberá ser propiedad del INMEGEN, así como ser registrada en la Biblioteca Única de Software; la cual estará físicamente en un almacén acondicionado para este propósito, o en su caso el resguardo de las credenciales de acceso estará a cargo de la Subdirección de Tecnologías de la información.

b) Es atribución de la Subdirección de Tecnologías de la Información dictaminar técnicamente las necesidades de Software del INMEGEN.

c) Con el fin de garantizar el correcto desempeño y administración del licenciamiento. Es facultad exclusiva de la Subdirección de Tecnologías de la Información realizar la instalación de Software en los equipos de cómputo propiedad INMEGEN.

d) La instalación de software a equipos de cómputo propiedad del INMEGEN se realizará exclusivamente con Licencias propiedad del instituto y bajo ninguna circunstancia se instalarán licencias propiedad del usuario final o de alguna otra entidad. Excepción a este artículo serán las licencias de prueba (Shareware) o libres (Free Software y los que sean autorizados.

e) La instalación de Software especializado deberá contar con la aprobación del Director del Área solicitante, a través de correo electrónico o ticket de servicio a la mesa de ayuda de Tecnologías de la información debiendo incluir la justificación del requerimiento.

f) La instalación de software en servidores de supercómputo de la Dirección de Investigación, El equipo de cómputo científico (cómputo científico conectado a dispositivos biomédicos) y desarrollo de software, será regido por los instrumentos establecidos por las Subdirecciones de Bioinformática, Secuenciación y Genotipificación y Análisis de Expresión en la normateca Institucional en concordancia a lo establecido por Coordinación de Estrategia Digital Nacional.

III. Sobre la navegación en Internet.

a) El navegador de internet avalado por la Subdirección de Tecnologías de la Información del INMEGEN es Google Chrome, debido a que es el que mejor opera con el correo electrónico institucional y la suite ofimática.

b) El acceso a los servicios de la Intranet, así como del internet, deberá ser exclusivamente con fines laborales de acuerdo a las necesidades del área en la que labora.

c) Está prohibida la navegación en sitios web que no tenga que ver con la naturaleza de sus actividades institucionales, además de los siguientes contenidos:

1. Pornografía.

2. Descarga ilegal de información o software de cualquier tipo que contravenga la Ley Federal de Derechos de Autor.

3. Usar el servicio de internet para fines diferentes al desempeño de sus funciones y atribuciones, así como con fines comerciales y personales.

4. Ingresar a sitios con contenido de armas, drogas, gaming, violencia o que represente un riesgo para la seguridad de la información pudiendo propiciar la propagación de malware en la red LAN.

5. Bajar, reproducir, contenido multimedia de internet, ya que estas acciones no están relacionadas con las actividades del instituto y puede representar un riesgo a la Seguridad de la Información pudiendo propiciar la propagación de malware en la red LAN

6. Visitar sitios web relacionados con minería de datos como criptomonedas.

7. Sitios web relacionados a hacking y/o evasión de seguridad de red, ataques a sistemas, entre otros.

d) Al detectar que un usuario final visite sitios con contenido inusual, ilícito o que ponga en riesgo la Seguridad de la Información del INMEGEN, se dará un aviso al involucrado y se anotará la observación correspondiente en la bitácora de accesos por usuario final. Además, se notificará por medio de un reporte a su superior inmediato y a la Subdirección de asuntos Jurídicos a fin de se que proceda conforme a derecho.

e) Únicamente serán dados de alta, laptops y/o tabletas con el registro correspondiente en la Subdirección de Tecnologías de la Información y la firma del formato que ésta emita.

f) Todo activo de tecnologías de la Información y comunicación que por sus características lo permita, deberá poseer una solución antivirus y antimalware actualizada antes de integrarse a la red institucional.

g) La navegación a internet en el interior del Instituto será de acuerdo a perfiles de usuarios que la Subdirección de Tecnologías de la Información estime conveniente.

h) Para la publicación de dominios internos y/o externos, así como la asignación de puertos específicos de red, deberá solicitarse a través de la Mesa de Ayuda de Tecnologías de la Información, integrando el nombre del servicio, puerto, dirección de origen, dirección destino, ya sea pública y/o privada.

i) La Subdirección de Tecnologías de la Información es la única facultada para bloquear todos aquellos sitios que se consideran un riesgo para la red de datos y que no sean compatibles con las labores de los usuarios finales.

j) En caso de requerir alguna excepción al punto anterior, el jefe inmediato deberá presentar una solicitud por escrito, informando a su director de área a través del correo electrónico institucional o ticket de servicio en la Mesa de Ayuda de TI.

k) Solo los equipos Institucionales podrán contar con el servicio de acceso a Internet, salvo las excepciones autorizadas por el Director General.

IV. Sobre el Correo Electrónico Institucional.

Con el fin de mejorar el intercambio de la información que se requiera o genera en el instituto, se pone a disposición de los usuarios finales que así lo determinen sus actividades, una herramienta tecnológica oficial con una capacidad finita de almacenamiento compartida entre todos los servicios en la nube que se incluya, la cual, le será asignada a petición del jefe inmediato o superior jerárquico con nivel mínimo de Jefatura, así como se deberá contar con

notificación de la Subdirección de Recursos Humanos. Cada usuario final debe observar lo siguiente:

a) Queda prohibido el uso del correo electrónico institucional del INMEGEN para:

1. Envío de correos masivos, cadenas o publicidad no relacionada al INMEGEN.
2. Suscribir la cuenta en sitios web sociales, comerciales, bancaria, de entretenimiento o cualquiera que no sea objeto de sus funciones.
3. Intercambiar cualquier material que transgreda la Ley Federal del Derecho de Autor.
4. Divulgar sus credenciales de acceso
5. Usar palabras o referencias que puedan resultar difamatorias, hostiles, ilegales, discriminatorias u ofensivas.
6. Reenvío de información a cuentas fuera del dominio institucional (.gob, .edu u .org)[2].
7. Hacer uso de cuentas de correo que no sean institucionales para intercambio de información institucional.
8. Divulgar información en apego al acuerdo de confidencialidad celebrado entre el usuario final y el INMEGEN.

b) Es responsabilidad de cada Usuario,

1. Salvaguardar la seguridad de la información de los activos de tecnologías de la información y comunicación bajo su resguardo.
2. Depurar la cuenta de correo electrónico que le fue asignada, a fin de evitar saturación e interrupción del servicio, privilegiando la conservación de activos esenciales de información
3. Supervisar los mecanismos adecuados en la información que se comparte.
4. Verificar que los dominios o información que reciba sean genuinos.

[2] **El Instituto tiene cuentas con dominio inmegen.gob.mx, para personal administrativo y de staff; cuentas con dominio inmegen.edu.mx, para Investigadores y estudiantes y el dominio inmegen.org se utiliza sobre todo para cuestiones de identificación del Instituto como centro de enseñanza.**

5. Atender que la información enviada y/o recibida, no supere los 25 Mb de tamaño y en su caso comprimir la información.

6. Verificar que la información enviada no contenga archivos maliciosos.

7. El área responsable tiene 30 días naturales para indicar las acciones a realizar con la cuenta de correo electrónico institucional.

c) La generación de una cuenta de correo electrónico, tendrá las siguientes características:

1. Creado con la inicial del nombre y el primer apellido.

2. En caso de que ya exista una cuenta con características similares se tomará en cuenta, si es el caso, la inicial de segundo nombre, y el segundo apellido.

d) La asignación de cuentas de correo electrónico será de acuerdo con el tipo de relación laboral que se celebre con el Instituto:

Dominio de correo electrónico	**Tipo de personal**
@inmegen.edu.mx	● Servicios Profesionales. ● Estudiantes. ● Investigadores Externos. ● Investigadores Catedráticos. ● Convenios Institucionales ● Interinatos ● Eventual.
@inmegen.gob.mx	● Apoyo Administrativo ● Soporte Administrativo ● Enlace ● Jefaturas ● Subdirecciones ● Oficina de Representación ● Direcciones de Área. ● Dirección General.

V. Sobre uso de telefonía.

a) La Subdirección de Tecnologías de la Información asignará equipo telefónico al usuario final que su jefe superior inmediato determine necesario para el ejercicio de las funciones encomendadas y de acuerdo a la disponibilidad de dispositivos al momento de la solicitud. Deberá realizarse por medio de una petición debidamente justificada y canalizada a la Mesa de Ayuda de Tecnologías de la Información para su procesamiento.

b) La asignación de permisos de marcación será acorde a lo siguiente:

Asignación de Permisos de Marcación	
Puesto	**Permisos**
Director General y Directores de Área	• Larga distancia internacional • Larga distancia nacional • Números locales • Números a celular • Extensiones telefónicas
Subdirectores	• Larga distancia nacional • Números locales • Números a celular • Extensiones telefónicas
Jefes de Departamento	• Números locales • Extensiones telefónicas
Asistentes y Personal Operativo	• Extensiones telefónicas

c) En caso de que un usuario final requiera permisos de marcación adicionales a los asignados de acuerdo con los criterios citados en la tabla "asignación de permisos de marcación", deberán ser solicitados de acuerdo al inciso a) de esta sección.

d) Evitar hacer uso del servicio telefónico para fines distintos a las actividades sustantivas y operativas del INMEGEN.

e) No modificar cualquier configuración del equipo telefónico.

f) En caso de algún incidente con el equipo telefónico, el resguardante deberá ponerse en contacto con la Mesa de Ayuda de Tecnologías de la Información a través de los diferentes canales de contacto, para generar una orden de servicio, así como registrar y otorgar los últimos 4 dígitos del número de serie y/o inventario.

g) En caso de requerir alguna configuración específica en la extensión telefónica asignada, el resguardante deberá solicitarla a través de los distintos canales de la

Mesa de Ayuda de Tecnologías de la Información, proporcionando adicionalmente los últimos cuatro dígitos del número de serie o inventario.

h) La Subdirección de Tecnologías de la Información, se reserva el derecho de suspender el uso atípico del servicio de voz en las extensiones telefónicas, así como notificar al resguardante y su jefe superior inmediato.

VI. Sobre los respaldos de información.

a) Todo Activo de Información es propiedad del INMEGEN; las personas servidoras públicas o usuarios finales que por sus funciones administren, generen y/o gestionen, serán los responsables de garantizar la seguridad de la información de los activos desde su creación hasta su destrucción. En este último caso (destrucción) es necesario contar con la autorización de la Dirección General o a quién está confiera.

b) Es responsabilidad del usuario final almacenar la información en los que cuenten con esta característica y estén bajo su resguardo.

c) Los respaldos de en cualquier medio físico pueden ser solicitados por el usuario final que figure como responsable a través de correo electrónico institucional o ticket de servicio a la Mesa de Ayuda de Tecnologías de la Información justificando su uso con visto bueno de la Dirección de Área y de acuerdo al inciso a) de la presente sección.

VII. Sobre el acceso remoto seguro.

El usuario final que por sus funciones requiera de un servicio de acceso remoto seguro a través de una red privada virtual (VPN), deberá solicitarlo, debidamente justificado, por escrito del Director del área a la Dirección de Administración, debiendo apegarse a lo siguiente:

i. Sólo los usuarios previamente autorizados podrán utilizar los beneficios del Acceso Remoto Seguro (VPN), los que, además, serán los responsables del correcto uso del servicio y sobre equipos de cómputo propiedad del Instituto y por periodo de tempo definido.

ii. Es de responsabilidad del usuario con privilegios VPN, asegurarse que ninguna otra persona utilice su cuenta de acceso, entendiendo que es de uso exclusivo para quienes se les ha asignado dichos privilegios.

iii. Deberá mantener siempre la seguridad y confidencialidad de las credenciales para el uso del sistema VPN.

iv. Los accesos son controlados y monitoreados por la Subdirección de Tecnologías de la Información y será su atribución el restringirlos o quitarlos en caso de detectar una violación o comportamiento anómalo.

v. En caso de que un usuario solicite el acceso remoto seguro (VPN) para ser utilizado en un equipo de cómputo que no sea propiedad del Instituto, deberá ser por escrito de la Dirección de Adscripción del usuario a la Dirección de Administración, a efecto de que se revise si procede la autorización.

vi. En todos los casos, los usuarios que sean autorizados deberán de llevar los equipos de cómputo a la Subdirección de Tecnologías de la Información para la configuración de la VPN y le sea asignado su usuario y contraseña.

vii. En los casos que su periodo de autorización haya vencido, la Dirección correspondiente deberá solicitarlo nuevamente por escrito a la Dirección de Administración.

VIII. Sobre el desarrollo de Software:

a) El Desarrollo de Software, está supeditado al cumplimiento de iniciativas con software libre de preferencia, para lo cual deben de ser dictaminados por la Agencia de Transformación Digital y Telecomunicaciones, en ese sentido deberán de hacer una solicitud a la Subdirección de Tecnologías e la Información para coadyuvar en el envío de la solicitud.

b) En todo momento, el área o personal técnico desarrollador, deberá apegarse a las mejores prácticas en la materia conforme Proyecto abierto de seguridad de aplicaciones web.

IX. Sobre la Mesa de Ayuda de Tecnologías de la Información:

Con la finalidad de mantener el adecuado control de solicitudes de servicios e incidentes relacionados a la operación de la infraestructura de TIC's, se cuenta con una Mesa de Ayuda de Tecnologías de la Información:

a) Horario de operación de lunes a viernes de 8:00 a 18:00 horas.
b) Con tres medios de comunicación:
   - Extensión telefónica: 1979.
   - Correo: mesadeayuda@inmegen.gob.mx
   - A través de Intranet.

c) Para agilizar el registro, asignación, seguimiento y atención de los tickets, es indispensable proporcionar los datos que a continuación se describen:
   - Datos generales del usuario solicitante
   - (nombre, correo institucional, extensión, adscripción y ubicación)
   - Descripción breve del incidente (Ejem. “Problemas para imprimir”, “Falla con conexión a
   - red inalámbrica”, “Cambio de contraseña”, “Equipo no enciende”)
   - No. de serie (equipo arrendado) y/o No. de inventario (equipo propiedad del instituto) Información extra (Descripción detallada que nos facilite entender el requerimiento)

Con el número de ticket asignado se le dará seguimiento.

Artículo 13.- La Subdirección de Tecnologías de la Información podrá proveer al personal del INMEGEN, préstamo de activos de tecnologías de la Información con el objeto de facilitar el desempeño de sus actividades o comisiones asignadas, de acuerdo a la existencia y disponibilidad en el almacén.

I. Los activos de tecnológicos a considerar son los siguientes:

a) Laptop
b) Proyector
c) Teléfono
d) Cable de red (máximo 2 por usuario final)
e) Cable vga
f) Cable dvi
g) Adaptadores,
h) Cable corriente para monitor o gabinete

Artículo 14.- Para el servicio de préstamos de activos de tecnologías de la Información, el usuario final deberá considerar las siguientes directrices:

I. Solicitar el equipo que requiere en préstamo por lo menos 24 horas antes de que éste vaya a ser utilizado.

II. Las solicitudes urgentes deberán realizarse con al menos 4 horas hábiles de anticipación. En ambos casos, el préstamo de equipos estará sujeto a la disponibilidad de los mismos;

III. La solicitud se deberá realizar mediante la Mesa de Ayuda de Tecnologías de la Información del INMEGEN, por medio de un correo electrónico institucional a la dirección "mesadeayuda@inmegen.gob.mx", o vía telefónica llamando a la extensión 1979, proporcionando los siguientes datos:

a) Nombre completo del Usuario;
b) Área;
c) Extensión;
d) Ubicación, piso y área de uso del equipo;
e) Fecha y hora de inicio de préstamo;
f) Fecha y hora de devolución del préstamo;
g) Tiempo en que se utilizará el equipo;
h) Uso que se le dará;
i) Indicar si sale o no de las instalaciones.

IV. En cualquier caso, el Usuario deberá recoger y entregar el equipo personalmente, en sótano 1, en la Subdirección de Tecnologías de la Información, donde deberá firmar la recepción y devolución del equipo en el documento correspondiente.

V. En caso de sufrir extravío o robo, deberá indicar a la Subdirección de Tecnologías de la Información así como a la Subdirección de Asuntos Jurídicos para proceder con los trámites correspondientes en caso de reposición.

VI. Cumplir con el tiempo en que será utilizado el equipo a préstamo. En caso de requerir extender el tiempo de préstamo, deberá notificar a Mesa de Ayuda de Tecnologías de la Información por lo menos 30 minutos antes de que se concluya el tiempo solicitado. Dicha extensión de tiempo estará sujeta a disponibilidad derivada de solicitudes programadas previamente por otros usuarios finales.

Artículo 15.- Con respecto a los daños hacia los activos de tecnologías de la Información y comunicación propiedad o a cargo del Instituto, se deberá considerar lo siguiente:

I. El usuario final asumirá los costos de reparación o reposición que resulten del uso inadecuado de los activos de Tecnologías de la Información y comunicación que tenga a su resguardo, con independencia de cualquier otra sanción que corresponda.

II. Únicamente el personal de la Subdirección de Tecnologías de la Información está autorizado para revisar, evaluar o reparar cualquier activo tecnológico propiedad del Inmegen. Por ningún motivo podrá hacerlo el usuario final o personal diferente al autorizado.

IX. Sobre Seguridad de la Información.

Artículo 16.- Todo Usuario final será provisto de las cuentas de acceso y contraseñas necesarias para el uso de los sistemas de información y recursos relacionados con las tecnologías de la información y comunicaciones, de acuerdo con las funciones de su puesto.

Las contraseñas provistas para el acceso a los sistemas y recursos de Información, son de carácter temporal, por lo que el usuario final deberá actualizarlas en su primer inicio de sesión.

I. Con el fin de crear Contraseñas seguras, el Usuario deberá apegarse a los siguientes criterios de seguridad:

a) Construir contraseñas combinando caracteres alfabéticos (mayúsculas y minúsculas), dígitos y caracteres especiales.

b) Definir contraseñas con una longitud mínima de 10 caracteres.

c) Cambiar sus contraseñas cada 6 meses como mínimo. El sistema le solicitará el cambio, el cual deberá realizarse en dicho periodo, de lo contrario no le permitirá el acceso a los sistemas administrados y deberá solicitar el cambio de contraseña.

d) Evitar reutilizar contraseñas anteriores o que sean usadas para el acceso a sistemas o sitios de uso personal.

e) Salvaguardar la integridad, seguridad y confidencialidad de las credenciales de acceso otorgadas.

Artículo 17.- A fin de preservar la Integridad, disponibilidad y confidencialidad de la Información, generada, recibida, procesada, almacenada y compartida a través de sistemas, aplicaciones, arquitectura de red, bases de datos y del personal, en el Instituto Nacional de Medicina Genómica, se deberán atender las siguientes premisas:

A. Generar contraseñas seguras e independientes para cada software de al menos 10 carácteres alfanuméricos, incluyendo minúsculas, mayúsculas y caracteres especiales.

B. No tener visible, pegadas o compartir sus credenciales de acceso de los sistemas a los que se le haya otorgado acceso

C. En los sistemas y aplicaciones que por sus características lo permitan deberán hacer uso al menos de 2 factores de autenticación.

D. Los sistemas y aplicaciones deberán contemplar el test de Turing público y automático para distinguir a los ordenadores de los humanos (CAPTCHA).

E. Mantener actualizado el software de los endpoint.

F. Con el fin de evitar código malicioso, abstenerse de abrir con extensiones: *.exe, *.com, *.bat, *.cmd, *.cpl, *.pif, *.scr y *.vbs que no sea conocido por los diverso medios de intercambio de información institucional.

G. No instalar software ilegal o pirata, debido a que puede contener software malintencionado.

H. A fin de evitar fraudes, cerciorarse de la autenticidad del sitio web que le solicite información sensible.

I. Realizar un esquema de respaldos de acuerdo a las necesidades de cada área.

J. Confirmar la integridad de los respaldos de los generados. Limitar la apertura de puertos TCP/UDP a lo estrictamente necesario.

K. Desactivar o bloquear los puertos no utilizados en cada endpoint que sea empleado para publicar servicios web o de acceso remoto.

L. Las cuentas de correo electrónico institucional serán eliminadas sin posibilidad de recuperación cuando tengan inactividad y más de 30 días sin uso.

M. En caso de algún incidente de seguridad de la información, el usuario final dará aviso a la Subdirección de Tecnologías de la Información a través de los medios de contacto en la Mesa de Ayuda de Tecnologías de la Información, así como notificar a la Dirección de Administración, a la Subdirección de Asuntos Jurídicos y a la Dirección General del Instituto para determinar el tratamiento al incidente.

N. Ningún usuario puede acceder a los aplicativos, sistemas y bases de datos sin la autorización correspondiente.

O. Queda restringido el acceso a los cuartos de comunicaciones y al centro de datos a solicitud expresa a la Dirección de Administración o a la Subdirección de Tecnologías de la Información.

P. Los proveedores y personal externo que requieran conexión algún sistema de información y/o aplicativo, deberán de seguir los protocolos y procedimientos de la Subdirección de Tecnologías de la Información.

TRANSITORIOS

PRIMERO. Las presentes Reglas se aprobaron durante la XXXX Sesión Ordinaria 2026 del Comité de Mejora Regulatoria Interna del INMEGEN (COMERI), celebrada el XX de XXXXX de XXXX.

SEGUNDO: Las presentes Reglas entrarán en vigor al día siguiente de su publicación en la normateca del Instituto.

TERCERO: Se dejan sin efecto las Reglas internas de uso de Software, equipos y servicios de cómputo en el INMEGEN, aprobadas el día diez de diciembre del año dos mil dieciocho.

CUARTO: Quedan sin efecto las disposiciones administrativas que se opongan a lo establecido en las presentes Reglas.

Aprobado en la Ciudad de México, a XX de XXXX de XXXX