Políticas para la seguridad de los sistemas de datos personales en el Instituto Nacional de Medicina Genómica

2007

Políticas para la seguridad de los sistemas de datos personales en el Instituto Nacional de Medicina Genómica

Objetivo

Las presentes políticas tienen como propósito establecer las reglas que los usuarios de equipos y/o servicios de cómputo deberán observar en el uso y control de la Infraestructura Tecnológica que se les asigne en el Instituto Nacional de Medicina Genómica, esto con el fin de garantizar la seguridad, integridad y disponibilidad de los datos personales que se manejan en el INMEGEN.

Marco legal

Ley de los Institutos Nacionales de Salud.
Ley Federal de Transparencia y Acceso a la Información.
Estatuto Orgánico del Instituto Nacional de Medicina Genómica.
Lineamientos de Protección de Datos Personales.
Lineamientos de Protección y Seguridad de Datos Personales del Instituto Nacional de Medicina Genómica.
Lineamientos de Manejo y Conservación de Archivos de la Administración Pública Federal.
Lineamientos de Manejo y Conservación de Archivos del Instituto Nacional de Medicina Genómica.

Índice

POLÍTICAS

Capítulo I
Generalidades

1. Para efectos de estas políticas se utilizarán las siguientes definiciones:
   I. ***Equipo de cómputo:*** Sistema electrónico que permite el acceso y tratamiento de información de forma electrónica mediante programas y dispositivos periféricos.
   II. ***Usuario autorizado:*** Personal del INMEGEN que hace uso del equipo de cómputo

mediante un usuario y contraseña que le haya sido asignado por la Subdirección de Tecnología de la Información ya sea mediante interacción física con o de manera remota.

III. ***Usuario no autorizado:*** Persona que hace uso de equipo de cómputo o de la red del INMEGEN ya sea mediante interacción física con o de manera remota sin la autorización correspondiente del responsable de los mismos.
IV. ***Servidor:*** Equipo de cómputo dedicado al almacenamiento y procesamiento de información que provee servicios de información en la red del INMEGEN o en Internet.
V. ***Red inalámbrica:*** Sistema de comunicaciones que interconecta equipos de cómputo mediante ondas electromagnéticas.
VI. ***Concentrador de red:*** Sistemas electrónicos que interconectan y agrupan equipos de cómputo en redes.
VII. ***Red alámbrica:*** Sistema de comunicaciones que interconecta equipos de cómputo mediante cables y equipos concentradores.
VIII. ***Red del INMEGEN:*** Sistemas de comunicaciones que interconecta equipos de cómputo, servidores y equipos de telecomunicaciones en el Instituto Nacional de Medicina Genómica.
IX. ***Internet:*** Red internacional de servidores y equipos de cómputo de acceso público.
X. ***VLAN:*** Funcionalidad de los equipos concentradores de red que permite agrupar en redes lógicas independientes equipos de cómputo conectados el equipo concentrador.
XI. ***Sistema de encripción de datos:*** Programa de cómputo diseñado para codificar la información y así evitar el acceso no autorizado a la misma.
XII. **Contraseña fuerte:** Conjunto de caracteres usados para el acceso a un sistema que cuenta con letras mayúsculas, minúsculas y números con el fin de dificultar ataques combinatorios para tener acceso no autorizado a los sistemas.

Capítulo II
Sobre el desarrollo interno de sistemas de datos personales

1. Todos los sistemas de datos personales desarrollados en el INMEGEN deben contar con la capacidad de manejar usuarios y contraseñas para tener acceso a los mismos.

2. Todos los sistemas de datos personales desarrollados en el INMEGEN deben contar con un módulo de administración de usuarios con capacidad para agregar, borrar y modificar usuarios y contraseñas.

3. Todos los sistemas de datos personales desarrollados en el INMEGEN deben contar con un historial de modificaciones a los registros y usuarios responsables de las mismas.

4. Los sistemas de datos personales desarrollados en el INMEGEN deben ser desarrollados con herramientas de software libre bajo el sistema operativo Linux a menos de que exista una justificación técnica emitida por el titular de la Subdirección de Servicios Computacionales y Desarrollo de Software y avalada por la Dirección de Desarrollo Tecnológico.

5. Los sistemas de datos personales desarrollados en el INMEGEN deben hacer uso de sistemas de encripción durante el acceso a la información por parte de los usuarios.

Capítulo III
Sobre la adquisición de sistemas de datos personales

6. Todos los sistemas de datos personales adquiridos por el INMEGEN deben contar con la capacidad de manejar usuarios y contraseñas para tener acceso a los mismos.

7. Todos los sistemas de datos personales adquiridos por el INMEGEN deben contar con un módulo de administración de usuarios con capacidad para agregar, borrar y modificar usuarios y contraseñas.

8. Todos los sistemas de datos personales adquiridos por el INMEGEN contar con un historial de modificaciones a los registros y usuarios responsables de las mismas.

9. Se dará preferencia a la adquisición de sistemas de datos personales que ofrezcan uso de sistemas de encripción durante el acceso a la información por parte de los usuarios.

Capítulo III
Del resguardo de los servidores con sistemas de datos personales en el INMEGEN

10. Todos los servidores que contengan datos personales deberán ser resguardados en la unidad de supercómputo y tecnología de la información del INMEGEN.

Capítulo IV
Sobre las administración de los servidores con sistemas de datos personales

11. Será responsabilidad de la Subdirección de Servicios Computacionales y Desarrollo de Software aplicar las últimas versiones de actualizaciones de seguridad en los servidores que contengan sistemas de datos personales desarrollados por personal del INMEGEN.

12. Será responsabilidad del proveedor aplicar las últimas versiones de actualizaciones de seguridad en los servidores que contengan sistemas de datos personales adquiridos por el INMEGEN. Sin embargo, si la Subdirección de Servicios Computacionales y Desarrollo de Software identifica huecos de seguridad que puedan afectar a otros elementos de la red del Inmegen en estos servidores, se desconectarán de la red hasta que el proveedor realice las actualizaciones correspondientes y garantice la seguridad de los mismos.

13. Será responsabilidad de la Subdirección de Servicios Computacionales y Desarrollo de Software administrar los servidores que contengan sistemas de datos personales desarrollados por el INMEGEN.

14. Será responsabilidad de la Subdirección de Tecnología la Información mantener actualizada la base datos de definiciones de virus en los equipos de cómputo que accesen los sistemas de datos personales del INMEGEN con la última versión disponible.

Capítulo V
Sobre la seguridad de la red del INMEGEN y los equipos de computo

15. Los equipos de cómputo del INMEGEN son para uso exclusivo de usuarios autorizados.

16. Los usuarios deben cumplir con las Políticas de Uso de Software, Equipos y Servicios de Cómputo en el INMEGEN vigentes emitidas por la Dirección de Desarrollo Tecnológico.

17. Los equipos de cómputo que necesiten acceso a los sistemas de datos personales deberán estar en la misma VLAN que el servidor.

18. Todos los equipos de cómputo del INMEGEN deberán contar con un programa protector de pantalla que deshabilite el uso del equipo y que requiera el ingreso del usuario y su contraseña para su desbloqueo.

19. Los usuarios de los equipos de cómputo del INMEGEN deberán activar el programa protector de pantalla mientras no utilicen el equipo o abandonen su lugar de trabajo.

20. Los equipos de cómputo del INMEGEN deberán activar automáticamente el programa protector de pantalla después de 10 minutos de no ser utilizados.

21. Será responsabilidad de la Subdirección de Servicios Computacionales y Desarrollo de Software la instalación, mantenimiento y administración de sistemas cortafuegos en todos los accesos a la red del INMEGEN desde Internet u otras redes externas.

22. Será responsabilidad de la Subdirección de Servicios Computacionales y Desarrollo de Software la instalación, mantenimiento y administración de sistemas de filtrado de acceso (PROXY) en todos los accesos de la red del INMEGEN hacia Internet u otras redes externas.

23. En la medida de lo posible los servidores que contengan sistemas de datos personales deberán estar en una VLAN que contenga solamente los equipos de cómputo propiedad del INMEGEN asignados a usuarios autorizados de estos sistemas y/o estarán una red exclusiva de servidores protegida por un equipo cortafuegos.

24. En el centro de datos del INMEGEN y en todos los cuartos de telecomunicaciones del INMEGEN se utilizarán únicamente concentradores de red administrables con capacidad para un mínimo de 1000 VLANS para interconectar los equipos de la red alámbrica del INMEGEN.

25. Los equipos de cómputo que accesen la red del INMEGEN por medio de la red inalámbrica no tendrán acceso a los sistemas de datos personales.

26. Será responsabilidad de la Subdirección de Tecnología de la Información realizar la preparación inicial y el borrado de los equipos de cómputo que manejen datos personales.

27. Será responsabilidad de la Subdirección de Tecnología de la Información asegurarse que cada usuario de sistemas de datos personales tenga contraseñas "fuertes" en sus equipos y sistemas y que las contraseñas de administrador sean diferentes para cada pc.

Capítulo VI
Listado de software autorizado para computadoras den sitios de acceso restringido

28. El software autorizado para computadoras en sitios de acceso restringido es el siguiente:

- Sistema operativo con las más recientes actualizaciones de seguridad.
- Navegador oficial última versión establecido por la Subdirección de Tecnología de la Información u otro en casos técnicamente justificado y avalado por dicha subdirección.
- Aplicación libre de oficina openoffice.
- En caso de sistema operativo Windows deberá contar con un sistema de antivirus con la última versión disponible de la base de definiciones de virus.

Capítulo VII
Listado de software autorizado para servidores en sitios de acceso restringido

29. El software autorizado para servidores en sitios de acceso restringido es el siguiente:

- Sistema operativo con las más recientes actualizaciones de seguridad.
- En caso de sistema operativo Windows deberá contar con un sistema de antivirus con la última versión disponible de la base de definiciones de virus.
- Programa para ofrecer el servicio http apache con las últimas actualizaciones de seguridad y soporte para el lenguaje php y/o asp en caso de servidores Windows.
- Programa secure shell con las últimas actualizaciones de seguridad.
- Programa de base de datos con las últimas actualizaciones de seguridad.

Capítulo VIII
Sobre el software adicional

30. En caso de requerir software adicional se debe hacer una solicitud formal a la Dirección de Desarrollo Tecnológico por parte del director del área usuaria acompañado de un listado de tareas a realizar con el software y en caso de compra una justificación para la adquisición del mismo.

Capítulo IX
Sobre los respaldos de la información

31. Será responsabilidad del Departamento de Tecnología de la Información asignar a cada usuario interno que concentre archivos de datos personales en su equipo carpetas de red privadas para el almacenamiento y respaldo de los mismos.

32. Será responsabilidad del usuario interno almacenar los archivos con datos personales en

las carpetas privadas que le hayan sido asignadas por el departamento de tecnología de la información para este propósito.

33. Todos los respaldos de información en medio físico deberán ser solicitados por el usuario de manera escrita a la Subdirección de Tecnología de la Información.

34. Será responsabilidad de la Subdirección de Servicios Computacionales y Desarrollo de Software implementar la funcionalidad de respaldos automáticos diarios de la información en todos los sistemas de datos personales desarrollados en el INMEGEN.

TRANSITORIO

ÚNICO: Las presentes políticas necesitan para su adopción definitiva de la autorización de la Junta de Gobierno del Instituto.