Dirección Jurídica

Ciudad de México, a 18 de mayo de 2023.

MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Las medidas de seguridad son elementos de control que tiene el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información. En el caso de los datos personales, las medidas de seguridad se implementan a lo largo de su ciclo de vida para evitar que los datos sean expuestos, alterados o bloqueados por personas o entidades no autorizadas.

Las medidas de seguridad se clasifican por su naturaleza en:

- **Administrativas.-** Son elementos o acciones que enfocan generalmente a los roles y responsabilidades asignados a las personas, grupos de personas o entidades que intervienen en algún paso en el tratamiento de la información.

- **Físicas. -** Consisten en la implementación de procesos o modificación de tareas dentro de un proceso con el objetivo de garantizar la seguridad de la información. En la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) se establece que son el conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

- **Tecnológicas.-** La LGPDPPSO, las define cormo el conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

Con la finalidad de mantener un monitoreo y revisión de las medidas de seguridad, se contemplará de manera permanente lo siguiente:

1. Mantener actualizado el inventario de datos personales y de los sistemas de tratamiento de los mismos.

2. Realizar un monitoreo de los esquemas de Seguridad de los servicios de red.

3. Difusión de la información por medios electrónicos al personal del Instituto para garantizar el cumplimiento de las políticas en materia de protección de datos personales.

4. Acuerdos de confidencialidad o no revelación.

5. Restricción de acceso a la información.

6. Sistema de gestión de contraseñas a cargo de cada unidad administrativa.

7. Uso de herramientas y administración de sistemas.

8. Control de acceso al código fuente de los programas.

9. Dentro de las diversas medidas de seguridad físicas para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento se realizan las siguientes actividades:

    a) Prevenir el acceso no autorizado al perímetro del lugar en que se resguardan los datos personales en sus instalaciones físicas.

    b) Archiveros específicos para su resguardo y uso de cerraduras para su acceso.

    c) Prevenir el daño o interferencia a las instalaciones físicas, recursos e información.

    d) Protección de los recursos móviles, portátiles y cualquier soporte físico o electrónico, que pueda salir de las instalaciones del Instituto.

    e) Prever que los equipos que contienen o almacenan datos personales tengan un mantenimiento eficaz que asegure su disponibilidad, funcionalidad e integridad.

    f) Resguardo de la información de manera periódica.

    g) Acceso personal y restringido a bases compartidas.

10. Las unidades administrativas serán responsables del personal designado y el manejo que este realice de la información contenida en las bases compartidas, programas, plataformas y equipos que contengan datos personales.

11. Será responsabilidad de la unidad administrativa y de los usuarios respaldar la información institucional, así como aquellas que contenga datos personales y que tengan bajo su resguardo en los equipos de cómputo asignados, asegurando que estos respaldos se conserven íntegramente. La Unidad de Informática proporcionará las herramientas tecnológicas y asesoramiento para que los usuarios protejan y respalden la información antes señalada, realizando a su vez un aseguramiento de la información; sin embargo, el proceso empleado se encuentra supeditado a la Seguridad perimetral que la Dirección General de Tecnologías de la Información y Telecomunicaciones de la Secretaría de Cultura, implemente a nivel sector.

12. Al personal que se le asignen equipos y sistemas informáticos propiedad de la Institución, serán responsables de su buen uso y cuidado de la información, en el desempeño de las actividades propias al cargo.

13. Cada unidad administrativa deberá informar de manera inmediata a la Unidad de Informática, cualquier eventualidad en los programas, plataformas, bases compartidas, equipos de cómputo, dispositivos periféricos y de telecomunicaciones.

14. La Unidad de Informática deberá atender oportunamente las eventualidades reportadas por las unidades administrativas y en caso de que así aplique, solicitar la atención de las fallas por parte de los proveedores de equipos de cómputo, dispositivos periféricos y de telecomunicaciones. Dando correcto seguimiento, acompañamiento al personal de las unidades administrativas y vigilando en todo momento que se de solución a los reportes generados.

15. La Unidad de informática es la única instancia responsable para administrar los equipos y sistemas informáticos del Instituto, por lo cual, las unidades administrativas que requieran alguna instalación, configuración, actualización y/o cambio de software o hardware deberá solicitarlo a dicha Unidad. Además, será la única facultada para atender las eventualidades reportadas en los programas, plataformas, bases compartidas, equipos de cómputo, dispositivos periféricos y de telecomunicaciones.

16. La Unidad de Informática, en el ámbito de su competencia será responsable de mantener, operar, asegurar, mejorar la infraestructura de cómputo y telecomunicaciones; así como, de proponer acciones que permitan otorgar los servicios informáticos necesarios para que el Instituto cumpla con sus funciones.

17. Se proporcionará a los usuarios el acceso controlado a los servicios de Internet, que no representen riesgo a los equipos y sistemas informáticos, la productividad y/o disponibilidad de la red.

18. Las unidades administrativas deberán monitorear e informar oportunamente a la Unidad de Informática, respecto a aquellas copias, borrados o impresiones de documentos e información donde no se hayan otorgado los permisos explícitamente a los usuarios.

19. Las Unidades Administrativas deberán cuidar, monitorear y evitar que se Transgreda cualquier recurso informático, sistemas o sitios de telecomunicaciones a los que no se esté permitido acceder por parte de los usuarios que así hayan designado y en apego a las funciones que realiza.

20. Las Unidades Administrativas deberán cuidar, monitorear y evitar que se instalen o distribuyan softwares que no se encuentren licenciados para ser usados en los equipos de cómputo y sistemas del Instituto.

21. Únicamente la Unidad de informática podrá deshabilitar, desinstalar o modificar la operación del antivirus y herramientas de seguridad informática institucionales. De igual manera, se encargará de implementar y/o solicitar las herramientas de seguridad que sean necesarias para el cuidado y mantenimiento de la información, en apego a lo establecido por la Dirección General de Tecnologías de la Información y Telecomunicaciones de la Secretaría de Cultura.

22. Los usuarios que por motivos de sus actividades institucionales requieran del acceso a los recursos informáticos del Instituto desde una conexión remota y externa con un equipo de cómputo, deberán contar con la autorización del titular del área administrativa, solicitando y justificando ante la Unidad de informática, a fin de que sea configurado el acceso a través de un canal seguro.

23. La Unidad de Informática, es la única instancia autorizada para administrar los equipos de cómputo portátil del Instituto, por lo cual el usuario que requiera alguna instalación, configuración o cualquier cambio de software o hardware deberá solicitarlo a dicha Unidad.

24. Por el riesgo adicional al que los equipos portátiles de cómputo están expuestos, la Unidad de Sistemas dispondrá de la configuración de los sistemas para proteger la información mediante el cifrado de los medios de almacenamiento.

Las acciones a monitorear son las siguientes:

1. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras.

2. Las nuevas amenazas que podrían estar activadas dentro y fuera de la organización y que no han sido valoradas.

3. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.

4. Verificación y actualización de los servidores públicos con acceso a datos personales. Considerando que las áreas deberán hacer llegar la información sobre la continuidad del personal adscrito (bajas, altas y/o cambio del personal) a la Unidad de Informática.

5. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto que resulten en un nivel inaceptable de riesgo.

6. Cambio de accesos a bases de datos y bases compartidas en cierto periodo de tiempo, en virtud de las notificaciones que las áreas hagan llegar a la Unidad de Informática, de acuerdo con sus necesidades operativas.

7. Verificar se implementen y actualicen los mecanismos necesarios para respaldar la información institucional y que contenga datos personales almacenados, en caso de mantenimiento o reparación de los equipos de cómputo.

8. Verificar por cada unidad administrativa que, el uso de dispositivos periféricos y de almacenamientos externos como: Memorias USB, Teléfonos Celulares, discos duros se

encuentre autorizado, siempre y cuando obedezca a las actividades profesionales propias a cargo del personal.

9. Verificación y actualización de los quipos de cómputo de aquellos usuarios que requieran el acceso a otros servicios de Internet. La Unidad de Informática deberá contar con los oficios correspondientes emitidos por la Unidad administrativa, que justifique el acceso a los servicios requeridos.

10. Monitoreo, verificación y actualización de manera periódica de los equipos de cómputo portátiles por parte de la Unidad de Informática.

El Comité de Transparencia de la Secretaría de Cultura es el órgano colegiado encargado de garantizar y promover la Transparencia y el Acceso a la Información, así como el respeto, salvaguarda y protección de los derechos de acceso a la información y de protección de datos personales y sus actividades conexas, por lo que, el Instituto Nacional del Derecho de Autor como Órgano administrativo desconcentrado de dicha Secretaría, proporcionará a la Unidad de Transparencia la información contenida en el Documento de Seguridad para su previa aprobación del Comité de Transparencia, conforme a lo siguiente:

1. Revisar y analizar el informe presentado.
2. Emitirá el Dictamen que contendrá recomendaciones y de ser el caso requerimientos, precisando ambos casos, los plazos para la atención de los mismos y envío de las evidencias con la atención que corresponda.

De conformidad con lo ya señalado, y en apego artículo 36 de la LGPDPPSO el Instituto Nacional del Derecho de Autor realizó la actualización del Documento de Seguridad como resultado de un proceso de mejora continua, por lo que, se encuentra en espera del Dictamen de aprobación del Comité de Transparencia, una vez aprobado, se procederá a su publicación en la página oficial del Instituto: www.indautor.gob.mx