



**INSTITUTO NACIONAL  
DE ESTADÍSTICA Y GEOGRAFÍA**

**POLÍTICAS PARA LA SEGURIDAD DE LA  
INFORMACIÓN DEL INSTITUTO NACIONAL DE  
ESTADÍSTICA Y GEOGRAFÍA.**

**DIRECCIÓN GENERAL DE INTEGRACIÓN, ANÁLISIS E  
INVESTIGACIÓN.**

**DICIEMBRE, 2014.  
Aguascalientes, Aguascalientes.**

**ÍNDICE:**

	<b>Pág.</b>
<b>INTRODUCCIÓN</b>	4
<b>I. GLOSARIO</b>	5
<b>II. OBJETO Y ÁMBITO DE APLICACIÓN</b>	8
<b>III. MARCO JURÍDICO</b>	8
<b>IV. POLÍTICAS GENERALES</b>	9
A. Protección de la Información	9
B. Propiedad de la Información	10
C. Mejora de los controles para la conservación y resguardo de la Información	10
D. Protección de los Datos personales	10
<b>V. POLÍTICAS ESPECÍFICAS</b>	11
<b>A. Sistema de Seguridad de la Información</b>	11
a.1. Fortalecimiento de la Seguridad de la Información en los procesos y servicios	11
a.2. Factores del Sistema de Seguridad de la Información	11
<b>B. Seguridad en el factor humano</b>	12
b.1. Inducción a la Seguridad de la Información y Principios Institucionales de Seguridad de la Información	12
b.2. Cambio de funciones de los servidores públicos del Instituto	12
b.3. Concientización a los servidores públicos del Instituto	13
b.4. Conclusión de la relación laboral de los servidores públicos del Instituto	13
<b>C. Seguridad física y ambiental</b>	13
c.1. Condiciones eléctricas y ambientales	13
c.2. Seguridad y control de acceso físico a los centros de cómputo e instalaciones de cableado	14
c.3. Control de acceso físico a las oficinas e instalaciones del Instituto	14
<b>D. Seguridad de comunicaciones y operaciones; acceso lógico y sistemas de Información</b>	14
<b>E. Administración de incidentes de Seguridad de la Información</b>	15
e.1. Reporte de incidentes de Seguridad de la Información	15
e.2. Tratamiento y administración de incidentes de Seguridad de la Información	15
<b>F. Continuidad de las operaciones</b>	15



<b>G. Cumplimiento legal</b>	15
<b>H. Organización de la Seguridad de la Información</b>	16
h.1. El Comité del Sistema de Seguridad de la Información	16
h.2. Atribuciones del Comité del Sistema de Seguridad de la Información	17
h.3. Grupo de Apoyo del Sistema de Seguridad de la Información	17
h.4. Enlace de Seguridad de la Información	18
h.5. Facilitador de Seguridad de la Información	19
<b>I. Responsabilidades y Sanciones</b>	19
<b>VI. INTERPRETACIÓN</b>	20
<b>TRANSITORIOS</b>	20

## INTRODUCCIÓN.

El Instituto Nacional de Estadística y Geografía (Instituto) es el organismo público con autonomía técnica y de gestión, personalidad jurídica y patrimonio propios facultado por el Estado Mexicano para generar información estadística y geográfica del país, coordinar el Sistema Nacional de Información Estadística y Geográfica (Sistema), así como operar el Servicio Público de Información y otros productos y servicios que resultan importantes para la toma de decisiones en el país.

El Instituto es un organismo que lleva a cabo distintos proyectos nacionales para proveer Información de calidad, pertinente, veraz y oportuna todo ello en un entorno de gran complejidad, lo que le ha permitido ser una institución pública que cuenta entre sus más valiosos activos con la confianza y credibilidad que la sociedad le confiere.

En este sentido, resulta primordial maximizar los esfuerzos y recursos en lo que se refiere a mantener segura la Información que el Instituto capta, produce, actualiza, organiza, procesa, integra, compila, publica, divulga y conserva.

En el Instituto se maneja Información estadística y geográfica, así como aquella propia de la gestión administrativa, siendo necesario reforzar los controles de seguridad para protegerla, independientemente de la forma en la que ésta se soporte.

La Seguridad de la Información no es un tema nuevo en el Instituto, nació quizás con él mismo, en el momento en el que cada responsable de proceso estableció acciones para proteger la Información, sin embargo, es necesario implementar acciones bajo una concepción sistémica, para lo cual se requiere la participación de toda la comunidad del Instituto.

El Sistema de Seguridad de la Información, con base en estándares nacionales e internacionales, como el MAAGTICSI y la familia de normas ISO/IEC 27000 así como en la teoría de los sistemas viables, busca coordinar las acciones orientadas a fortalecer la seguridad de la Información en el Instituto, privilegiando la concientización del personal, para fortalecer el ambiente de seguridad donde cada trabajador actúa de manera convencida y comprometida con el resguardo de la Información institucional.

Es importante que las acciones de seguridad de la Información sean adoptadas como actividades propias de los procesos de trabajo, en lugar de ser vistas como algo adicional, como responsabilidad de terceros o de los mecanismos tecnológicos; ello refuerza la importancia de que la prioridad del Sistema de Seguridad de la Información sean los servidores públicos.

Con el fin de establecer y definir las pautas de operación del Sistema de Seguridad de la Información y con fundamento en lo dispuesto por los artículos 26, apartado B de la Constitución Política de los Estados Unidos Mexicanos, 66 y 77 fracción XIV de la Ley del Sistema Nacional de Información Estadística y Geográfica y 5 fracción XIV del Reglamento Interior del Instituto Nacional de Estadística y Geografía, los miembros de la Junta de Gobierno han tenido a bien emitir las siguientes:

## **POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA**

### **I. GLOSARIO.-**

Para efectos de las presentes Políticas se entenderá por:

- 1. Activo de Información:** Toda aquella Información y medio que la contiene, que por su importancia y el valor que representa para el Instituto, deben ser protegidos para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue;
- 2. Activo de Información clave:** El Activo de Información que resulta esencial o estratégico para la operación y/o el control de una Infraestructura crítica o incluso de una que no tenga este carácter, pero cuya destrucción, pérdida, alteración o falla tendría un grave impacto o consecuencia en la funcionalidad de la infraestructura o en los servicios que soporta en el Instituto;
- 3. Activo de TIC:** Los programas de cómputo, bienes informáticos, soluciones tecnológicas, sistemas o aplicativos y sus componentes, las bases de datos o archivos electrónicos;
- 4. Áreas Administrativas:** Las Direcciones Generales Adjuntas adscritas a las diversas Unidades Administrativas del Instituto, incluidas las Direcciones Regionales y las Coordinaciones Estatales del mismo;
- 5. Comité:** El Comité del Sistema de Seguridad de la Información;



6. **Confidencialidad:** Atributo de Seguridad de la Información que indica que la información sólo es revelada a individuos autorizados;
7. **Control de Seguridad:** Medidas, procedimientos o acciones tendientes a evitar la ocurrencia o corregir el impacto de los riesgos;
8. **Datos personales:** Información concerniente a una persona física, identificada o identificable, entre otras, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva, familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias y convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad;
9. **Disponibilidad:** Atributo de Seguridad de la Información que consiste en que la información puede ser accedida por el personal cuando éste lo requiere;
10. **Enlace Informático:** El servidor público designado por el Titular de cada unidad administrativa, como responsable para apoyar y acordar con la Dirección General Adjunta de Informática todo lo relacionado con la coordinación de la función informática al interior de la unidad administrativa de su adscripción;
11. **Enlace de Seguridad de la Información:** Servidor público del Instituto, designado por el Titular de cada unidad administrativa como su representante ante el Comité;
12. **Facilitador:** Servidor público del Instituto designado por el Titular de cada unidad administrativa para impartir los talleres determinados por el Comité;
13. **Grupo de Apoyo:** Grupo de servidores públicos del Instituto que apoyan al Director General de Integración, Análisis e Investigación en la coordinación del Sistema de Seguridad de la Información;
14. **Grupo Técnico:** Equipo multidisciplinario conformado al interior de las Unidades Administrativas, con el objetivo de desarrollar el análisis correspondiente para el fortalecimiento de la Seguridad de la Información en los procesos y servicios de su competencia;
15. **Incidente de Seguridad de la Información:** Hecho que sucede de manera inesperada, materializando un riesgo que afecta a la Seguridad de la Información;
16. **Información:** Comprende la Información estadística y geográfica en términos de lo previsto por las fracciones III y IV, del artículo 2 de la Ley del Sistema Nacional de Información Estadística y Geográfica, así como aquella propia de la gestión administrativa del Instituto;



17. **Infraestructura crítica:** instalaciones, redes, servicios y equipos asociados o vinculados con Activos de TIC o Activos de Información del Instituto, cuya afectación, tendría un impacto mayor, entre otros, en la salud, la seguridad, el bienestar de los servidores públicos o en el eficaz funcionamiento del Instituto por lo que hace al cumplimiento de sus objetivos;
18. **Instituto:** Instituto Nacional de Estadística y Geografía;
19. **Integridad:** Atributo de Seguridad de la Información referente a que la información está completa y sin alteraciones;
20. **Personal Externo:** Personal de otras instituciones u organismos y los estudiantes, que realizan labores, estancias, prácticas profesionales y servicio social en el interior del Instituto;
21. **Prestadores de Servicios:** Personal de empresas proveedoras de servicios que realizan labores en el interior del Instituto;
22. **Proceso:** Conjunto de actividades que interactúan entre sí, las cuales transforman elementos de entrada en resultados;
23. **Reglamento:** Reglamento Interior del Instituto Nacional de Estadística y Geografía;
24. **Responsable de Proceso:** Servidor público encargado de coordinar las actividades para la realización de un proceso o proyecto relacionado con la producción de Información, la generación de productos o la prestación de servicios;
25. **Riesgo o Riesgo de Seguridad de la Información:** Es el efecto de la incertidumbre respecto al mantenimiento de la Seguridad de la Información en el Instituto;
26. **Seguridad de la Información:** Capacidad de preservar la confidencialidad, Integridad y disponibilidad de la Información a partir de la implementación de medidas técnicas y organizativas;
27. **Sistema de Seguridad de la Información:** Conjunto de normas, políticas, funciones, procesos y procedimientos que contribuyen a preservar la confidencialidad, integridad y disponibilidad de la Información;
28. **TIC:** Tecnologías de Información y Comunicaciones;
29. **Unidades Administrativas:** La Junta de Gobierno del Instituto y la Presidencia, las Direcciones Generales y la Contraloría Interna del Instituto, a que hacen referencia los artículos 3, 4, 5, 8, 9 y 47 del Reglamento Interior del Instituto Nacional de Estadística y Geografía.

## II. OBJETO Y ÁMBITO DE APLICACIÓN.-

Establecer la política institucional en materia de Seguridad de la Información para aplicar las medidas de índole administrativa, física y técnica que permitan mantener la confidencialidad, integridad y disponibilidad de la Información.

Las presentes Políticas son de observancia general y obligatoria para las Unidades y Áreas Administrativas del Instituto y los servidores públicos adscritos a las mismas.

## III. MARCO JURÍDICO.-

### a) Constitución Política de los Estados Unidos Mexicanos.

### b) Leyes.

- b.1. Ley del Sistema Nacional de Información Estadística y Geográfica;
- b.2. Ley Federal del Derecho de Autor;
- b.3. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;
- b.4. Ley Federal de Archivos;
- b.5. Ley de la Propiedad Industrial;
- b.6. Ley Federal de Responsabilidades Administrativas de los Servidores Públicos, y
- b.7. Código Penal Federal.

### c) Reglamentos.

- c.1. Reglamento de la Ley de la Propiedad Industrial;
- c.2. Reglamento de la Ley Federal del Derecho de Autor;
- c.3. Reglamento de Transparencia y Acceso a la Información Pública del Instituto Nacional de Estadística y Geografía, y
- c.4. Reglamento Interior del Instituto Nacional de Estadística y Geografía.

### d) Normas.

- d.1. Norma para el Acceso, Difusión y Promoción de la Información Estadística y Geográfica que genera el Instituto Nacional de Estadística y Geografía, y
- d.2. Normas de Control Interno para el Instituto Nacional de Estadística y Geografía.



**e) Políticas.**

- e.1. Políticas para la seguridad informática;
- e.2. Políticas para el Desarrollo de Sistemas Informáticos, y
- e.3. Políticas para la Administración y uso de Servicios Tecnológicos.

**f) Reglas.**

- f.1. Reglas de Operación del Laboratorio de Análisis de Datos del INEGI.

**g) Lineamientos.**

- g.1. Lineamientos de cambios a la Información divulgada en las publicaciones estadísticas y geográficas del Instituto Nacional de Estadística y Geografía;
- g.2. Lineamientos generales para la administración y uso de las Tecnologías de Información y Comunicaciones en el INEGI;
- g.3. Lineamientos para el uso y portación de la credencial de identificación del Instituto Nacional de Estadística y Geografía;
- g.4. Lineamientos para la elaboración de acta entrega recepción de los servidores públicos del Instituto Nacional de Estadística y Geografía;
- g.5. Lineamientos para la organización y conservación de los archivos del Instituto Nacional de Estadística y Geografía, y
- g.6. Lineamientos para la ventanilla única de recepción documental y la administración de los expedientes del personal.

**IV. POLÍTICAS GENERALES.-**

**A. Protección de la Información:**

Todos los servidores públicos del Instituto son responsables de conservar y resguardar la Información que por razón de su empleo, cargo o comisión, tengan bajo su cuidado, sea Información estadística, geográfica o de la gestión administrativa, generada por el Instituto o entregada por terceros; así mismo deben aplicar los mecanismos de protección establecidos por los responsables de los procesos y así como aquellos que se determinen en el marco del Sistema de Seguridad de la Información, para brindar la protección de la confidencialidad, integridad y disponibilidad de la Información.

### **B. Propiedad de la Información:**

La Información generada en el Instituto pertenece a éste, a menos que mediante un instrumento legal se establezca lo contrario, en cuyo caso deberá estarse al contenido del mismo en términos de las disposiciones legales y normativas que resulten aplicables, sin embargo, la facultad de otorgar acceso a la Información corresponde al Responsable del proceso en la Unidad Administrativa competente.

### **C. Mejora de los controles para la conservación y resguardo de la Información:**

Conforme a lo establecido en el Reglamento, en los artículos 14 fracciones III y XX, 18 fracciones IV y XXI, 19 fracciones V y XXII y 24 fracciones I y XXX, corresponde a la Dirección General de Coordinación del Sistema Nacional de Información Estadística y Geográfica en coordinación con la Dirección General de Estadísticas Sociodemográficas, la Dirección General de Estadísticas Económicas, la Dirección General de Estadísticas de Gobierno, Seguridad Pública y Justicia, y la Dirección General de Geografía y Medio Ambiente, definir los mecanismos para la conservación y resguardo de la Información estadística y geográfica, o bien documentar los existentes. Tratándose de aspectos relacionados con aplicación o uso de activos de Tecnologías de la Información y Comunicaciones, las Unidades Administrativas se coordinarán con la Dirección General Adjunta de Informática para su definición. En el caso de la Información propia de la gestión administrativa del Instituto, se realizará conforme lo establecido en las disposiciones normativas que regulen la organización y conservación de los archivos del Instituto.

En estos casos, es competencia del Comité, en coordinación con las Unidades y las Áreas Administrativas responsables de la Información, establecer las acciones tendientes a mejorar los controles de Seguridad de la Información. En este contexto, para el caso específico de la información propia de la gestión administrativa del Instituto, el Comité escuchará la opinión de las diversas instancias previstas por el Reglamento de Transparencia y Acceso a la Información Pública del Instituto Nacional de Estadística y Geografía.

### **D. Protección de los Datos personales:**

Todo dato personal debe ser tratado como confidencial de conformidad con las disposiciones legales y normativas aplicables en el Instituto.

Para la protección de la Información estadística y geográfica corresponderá a cada Unidad Administrativa, en su ámbito de competencia, establecer mecanismos que garanticen de manera particular la confidencialidad de los datos personales de los informantes, en las actividades de captación, producción, actualización, organización, procesamiento, integración, compilación, publicación, divulgación, conservación y destrucción, en cumplimiento a lo previsto por la Ley del Sistema Nacional de Información Estadística y Geográfica.

Para la protección de los datos personales contenidos en la Información propia de la gestión administrativa del Instituto, se deberá estar a lo establecido por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y el Reglamento de Transparencia y Acceso a la Información Pública del Instituto Nacional de Estadística y Geografía, de conformidad con lo dispuesto por el artículo 47 de la Ley del Sistema Nacional de Información Estadística y Geográfica.

## V. POLÍTICAS ESPECÍFICAS.-

### A. Sistema de Seguridad de la Información:

Se entiende por Sistema de Seguridad de la Información al conjunto de normas, políticas, funciones, procesos y procedimientos que, de manera coordinada, contribuyen a preservar la confidencialidad, integridad y disponibilidad de la Información bajo resguardo del Instituto.

#### a.1. Fortalecimiento de la Seguridad de la Información en los procesos y servicios:

La mejora continua de la Seguridad de la Información en los procesos y servicios institucionales, establecidos en la Estrategia General de Seguridad de la Información, se atenderá conforme la aplicación de la metodología prevista en los Lineamientos para el Fortalecimiento de la Seguridad de la Información en los procesos y servicios institucionales.

#### a.2. Factores del Sistema de Seguridad de la Información:

Para la implementación del Sistema de Seguridad de la Información se deberán tomar en cuenta los siguientes factores:

1. Los objetivos y acciones del Sistema de Seguridad de la Información deberán estar alineados con las atribuciones del Instituto;
2. El apoyo y compromiso de los mandos superiores y medios del Instituto;



3. La realización de acciones tendientes a diseminar el conocimiento en materia de Seguridad de la Información entre los servidores públicos del Instituto;
4. La difusión de la cultura de la Seguridad de Información orientada a elevar el nivel de conciencia de los servidores públicos del Instituto, el personal externo y los prestadores de servicios que por motivo de las funciones que desarrolle esté en contacto con algún activo de Información, y
5. La implementación de un sistema de medición para evaluar los resultados de la Seguridad de la Información que permita la mejora continua.

## **B. Seguridad en el factor humano.-**

### **b.1. Inducción a la Seguridad de la Información y Principios Institucionales de Seguridad de la Información:**

Las Unidades y Áreas Administrativas implementarán acciones para que los servidores públicos del Instituto de nuevo ingreso, así como el personal externo que por motivo de las funciones que desarrolle esté en contacto con algún activo de Información, sean orientados en las funciones que deben desempeñar y en el adecuado manejo de la Información del Instituto de acuerdo con las actividades que éstos llevan a cabo.

Así mismo, los servidores públicos del Instituto, deben firmar un acuerdo de aceptación de los Principios Institucionales de Seguridad de la Información. Lo señalado anteriormente debe ser aplicado por las áreas de administración de las Unidades y Áreas Administrativas, en coordinación con la Dirección General Adjunta de Recursos Humanos. Las Áreas Administrativas determinarán en su caso, cuando resulte necesario hacer extensivo el acuerdo de aceptación de referencia a Personal Externo y Prestadores de Servicios que colaboren con los servidores públicos en proyectos institucionales.

### **b.2. Cambio de funciones de los servidores públicos del Instituto:**

La Dirección General Adjunta de Recursos Humanos promoverá, entre las Direcciones de Administración de las Unidades y Áreas Administrativas, el uso de mecanismos para que cualquier cambio de adscripción que implique la reasignación de funciones a cargo de los servidores públicos del Instituto, así como del personal externo, se realice de una manera ordenada y controlada, de manera que no sustraigan información relacionada con su encargo anterior, con el fin de garantizar la Seguridad de la Información.

### **b.3. Concientización a los servidores públicos del Instituto:**

El Comité deberá supervisar la ejecución de las acciones de concientización descritas en el Programa Anual de Trabajo del Comité del Sistema de Seguridad de la Información, en el que se involucre a todos los servidores públicos del Instituto, para la protección de los Activos de Información y los Activos de TIC.

Los servidores públicos del Instituto, que por motivo de las funciones que desarrolle esté en contacto con algún Activo de Información, deben asistir a las sesiones de concientización que en materia de Seguridad de la Información se lleven a cabo en el Instituto, como parte de las acciones a seguir en materia de capacitación sobre Seguridad de la Información. Las Áreas Administrativas determinarán en su caso, cuando resulte necesario hacer extensiva la participación de Personal Externo y Prestadores de Servicios a las sesiones de concientización antes citadas.

### **b.4. Conclusión de relación laboral de los servidores públicos del Instituto:**

Los servidores públicos del Instituto que por motivo de sus funciones tenga acceso a los Activos de Información, al concluir la relación laboral con el Instituto no podrán conservar en su poder o sustraer Información del Instituto; pudiendo conservar exclusivamente aquella información que se integre al Acta de Entrega-Recepción y sus anexos debiendo entregar a su jefe inmediato o al servidor público que haya sido designado para tal efecto la Información institucional que tengan bajo su custodia.

## **C. Seguridad física y ambiental.-**

### **c.1. Condiciones eléctricas y ambientales:**

Las Unidades Administrativas en coordinación con la Dirección General Adjunta de Recursos Materiales y Servicios Generales, establecerán acciones que permitan el adecuado suministro de energía eléctrica y las condiciones medioambientales necesarias para la operación de los recursos informáticos. Además deberán contar con la documentación del diseño de las instalaciones de los componentes tecnológicos con que cuenta el Instituto, con el fin de poder realizar una adecuada planeación e implantación de controles para la Seguridad de la Información.

De igual manera, se deben prever los mecanismos que generen las condiciones medioambientales y los medios adecuados para el almacenamiento de documentos, considerando el aprovechamiento, optimización del mobiliario y espacios asignados para tal fin.

### **c.2. Seguridad y control de acceso físico a los centros de cómputo e instalaciones de cableado:**

Las Unidades Administrativas en coordinación con la Dirección General Adjunta de Informática y la Dirección General Adjunta de Recursos Materiales y Servicios Generales, establecerán acciones para una adecuada implantación de los mecanismos de seguridad y control de acceso físico a los centros de cómputo e instalaciones de cableado del Instituto.

### **c.3. Control de acceso físico a las oficinas e instalaciones del Instituto:**

La Dirección General Adjunta de Recursos Materiales y Servicios Generales, establecerá las medidas para controlar el acceso físico a las instalaciones del Instituto siendo responsabilidad de cada Unidad Administrativa su observancia y aplicación.

Las Unidades y Áreas Administrativas del Instituto en coordinación con la Dirección General Adjunta de Recursos Materiales y Servicios Generales, deberán identificar las oficinas y áreas consideradas como de acceso restringido y aplicar las medidas pertinentes para ello.

La Dirección General Adjunta de Recursos Materiales y Servicios Generales en coordinación con las Unidades Administrativas generarán y actualizarán un inventario de la Infraestructura crítica de los bienes inmuebles del Instituto, el cual deberá entregar al Comité en marzo de cada año y debe contener los siguientes datos: descripción, tipo de uso, ubicación, servidor público responsable y el nivel de criticidad para la operación del Instituto.

### **D. Seguridad de comunicaciones y operaciones; acceso lógico y sistemas de Información:**

En lo referente a la seguridad de las comunicaciones y operaciones, el control de accesos lógicos y la adquisición, desarrollo, uso y mantenimiento de los sistemas de Información, las Unidades y Áreas Administrativas del Instituto atenderán lo establecido por la Dirección General Adjunta de Informática en el marco de la seguridad informática, quien deberá considerar los siguientes aspectos:

1. Que la planeación, adquisición, desarrollo y aceptación de soluciones tecnológicas (sistema o aplicativos y sus componentes), asignación de responsabilidades y cambios en la tecnología

- aseguren la continuidad de las operaciones, la seguridad de los activos de TIC, la confidencialidad, integridad y disponibilidad de la Información y la documentación de los procesos, y
2. Que los mecanismos para el monitoreo, acceso, respaldo y protección de la Información, así como de la plataforma tecnológica, aseguren la confidencialidad, integridad y disponibilidad de la Información.

El Director General Adjunto de Informática en coordinación con las Unidades Administrativas, generarán y actualizarán un inventario de la Infraestructura Crítica y de los Activos de TIC que resultan necesarios para la operación y el control de los procesos y servicios informáticos del Instituto, el cual deberá entregar al Comité en marzo de cada año y debe contener los siguientes datos: descripción, tipo (telefonía, redes, aplicación, software, servicios), ubicación, servidor público responsable y nivel de criticidad para la operación del Instituto.

#### **E. Administración de incidentes de Seguridad de la Información.-**

##### **e.1. Reporte de incidentes de Seguridad de la Información:**

Todos los servidores públicos del Instituto están obligados a reportar cualquier incidente de Seguridad de la Información conforme al Protocolo que establezca el Comité.

##### **e.2. Tratamiento y administración de incidentes de Seguridad de la Información:**

Los responsables de procesos institucionales deberán dar seguimiento, en el ámbito de su competencia, de manera expedita a aquellos incidentes reportados y establecer las medidas necesarias para evitar que vuelvan a ocurrir, conforme al Protocolo que establezca el Comité.

#### **F. Continuidad de las operaciones:**

Las Unidades y Áreas Administrativas, en su ámbito de competencia, atenderán los incidentes de Seguridad de la Información que se presenten según la magnitud y grado de afectación de los mismos sobre el Instituto, debiendo realizar las acciones necesarias para restablecer las operaciones al menor costo y pérdidas posibles para el Instituto, manteniendo canales de comunicación entre los usuarios de los sistemas institucionales.

#### **G. Cumplimiento legal:**

Las Unidades y Áreas Administrativas del Instituto, con asesoría de la Dirección General Adjunta de Asuntos Jurídicos, se cerciorarán que las acciones que adopten para proteger los Activos de Información se apeguen a las disposiciones legales y normativas aplicables.

Los servidores públicos del Instituto, así como el Personal Externo, tienen la obligación de respetar la legislación concerniente a la protección de la Información, así como de los datos personales.

## **H. Organización de la Seguridad de la Información;**

La Seguridad de la Información es una responsabilidad institucional compartida, por ello el Instituto contará con un Comité del Sistema de Seguridad de la Información para realizar acciones tendientes a la coordinación de los trabajos que se emprendan por las Unidades Administrativas del Instituto en el fortalecimiento de la Seguridad de la Información.

### **h.1. El Comité del Sistema de Seguridad de la Información:**

El Comité del Sistema de Seguridad de la Información estará integrado de la siguiente manera:

1. El Director General de Integración, Análisis e Investigación, quien fungirá como Presidente;
2. El Enlace de Seguridad de la Información de cada Unidad Administrativa en calidad de Vocal;
3. El Director General Adjunto de Informática en calidad de Vocal;
4. El Director de Innovación y Tecnologías de la Información, adscrito a la Dirección General de Integración, Análisis e Investigación, como Secretario Ejecutivo, quien en ausencia del Presidente del Comité fungirá como Suplente,
5. La Contraloría Interna en calidad de asesor, y
6. Las direcciones generales adjuntas de Asuntos Jurídicos, Recursos Materiales y Servicios Generales, y Recursos Humanos, en calidad de asesores.

Los Vocales deberán contar con un nivel mínimo de Director de Área y deberán ser acreditados ante el Presidente del Comité por el Titular de la Unidad Administrativa de que se trate.

Los Asesores deberán contar con un nivel mínimo de Subdirector de Área y deberán ser acreditados ante el Presidente del Comité por el Titular de la unidad o área administrativa de que se trate.

El funcionamiento del Comité deberán apegarse a lo establecido en el Manual de Integración y



Funcionamiento del Comité del Sistema de Seguridad de la Información.

## **h.2. Atribuciones del Comité del Sistema de Seguridad de la Información:**

Son atribuciones del Comité:

1. Aprobar su Manual de Integración y Funcionamiento, así como sus actualizaciones;
2. Realizar acciones tendientes al diseño de la Estrategia General de Seguridad de la Información para el Instituto, así como efectuar su revisión al menos una vez al año;
3. Desarrollar el Programa Anual de Trabajo del Comité del Sistema de Seguridad de la Información;
4. Establecer y supervisar la aplicación de los Lineamientos para el Fortalecimiento de la Seguridad de la Información en los Procesos y Servicios Institucionales y el Protocolo Institucional de Respuesta a incidentes de Seguridad de la Información;
5. Conforme a las revisiones que se hagan al Sistema de Seguridad de la Información, proponer las mejoras correspondientes;
6. Promover la difusión y apoyo a la Seguridad de la Información en el Instituto;
7. Revisar el inventario de infraestructura crítica, de activos de información clave y de activos de Información del Instituto;
8. Promover el desarrollo y mantenimiento de planes de continuidad operativa en el Instituto frente a interrupciones imprevistas, y
9. Las demás que establezcan las presentes Políticas, el Manual de Integración y Funcionamiento del Comité y los Lineamientos para el Fortalecimiento de la Seguridad de la Información en los Procesos y Servicios Institucionales y demás disposiciones legales y administrativas aplicables.

## **h.3. Grupo de Apoyo del Sistema de Seguridad de la Información:**

Para facilitar la coordinación del Sistema de Seguridad de la Información, a cargo de la Dirección General de Integración, Análisis e Investigación, se conformará el Grupo de Apoyo del Sistema de Seguridad de la Información, el cual estará integrado por los titulares de la Dirección de Innovación y Tecnologías de la Información; la Subdirección de Seguridad de la Información; la Subdirección de Soluciones Informáticas; la Subdirección de Continuidad Operativa, todas ellas adscritas a la Dirección General de Integración, Análisis e Investigación, así como, los titulares de la Subdirección de Control y Evaluación A de la Contraloría Interna y de la subdirecciones de

Seguridad Informática y de Infraestructura Electromécanica de la Dirección General de Administración.

El Grupo de Apoyo del Sistema de Seguridad de la Información tendrá las siguientes funciones:

1. Desarrollar y proponer la actualización de la normatividad que regule la coordinación del Sistema de Seguridad de la Información;
2. Desarrollar y actualizar la metodología para el fortalecimiento de la Seguridad de la Información en los procesos y servicios del Instituto;
3. Proponer al Director General de Integración, Análisis e Investigación las acciones de concientización en materia de Seguridad de la Información;
4. Proponer al Comité, por conducto de su Presidente, los mecanismos para difundir el marco normativo a utilizar en el fortalecimiento de la Seguridad de la Información en los procesos y servicios;
5. Promover la difusión de la seguridad y el registro de incidentes de Seguridad de la Información en el Instituto, y
6. Las demás que establezcan las presentes Políticas, Lineamientos para el Fortalecimiento de la Seguridad de la Información en los Procesos y Servicios Institucionales y demás disposiciones administrativas aplicables.

#### **h.4. Enlace de Seguridad de la Información:**

Los vocales designados por los titulares de las Unidades Administrativas, fungirán como enlaces de Seguridad de la Información, quienes tendrán las siguientes funciones al interior de la Unidad Administrativa de su adscripción:

1. Contribuir en la aplicación de medidas y procedimientos determinados por el Comité;
2. Dirigir, conforme se establezca en los Lineamientos para el Fortalecimiento de la Seguridad de la Información en los Procesos y Servicios Institucionales, las etapas correspondientes al fortalecimiento de la Seguridad de la Información en los procesos y servicios;
3. Coordinar la integración de los grupos técnicos;
4. Proponer las actividades de capacitación de Seguridad de la Información de los facilitadores y grupos técnicos, para su inclusión en el programa de capacitación que integra la Dirección General Adjunta de Recursos Humanos
5. Integrar y resguardar la documentación y evidencias derivadas del fortalecimiento de la Seguridad de la Información en los procesos y servicios;



6. Enviar trimestralmente informes, al Grupo de Apoyo, sobre a los avances obtenidos en el fortalecimiento de la Seguridad de la Información en los procesos y servicios;
7. Plantear y promover en el Comité las inquietudes y propuestas para el Sistema de Seguridad de la Información que surjan de su área de adscripción;
8. Comunicar al Comité los incidentes de Seguridad de la Información que se presenten en la Unidad Administrativa de su adscripción, y
9. Las demás que establezcan las presentes Políticas, Lineamientos para el Fortalecimiento de la Seguridad de la Información en los Procesos y Servicios Institucionales y demás disposiciones administrativas aplicables.

#### **h.5. Facilitador de Seguridad de la Información:**

Los titulares de las Unidades Administrativas designarán por escrito a los servidores públicos del Instituto que fungirán como facilitadores de Seguridad de la Información, quienes tendrán las siguientes funciones al interior de la unidad administrativa de su adscripción:

1. Colaborar en las acciones necesarias para llevar a cabo la capacitación en materia de Seguridad de la Información a los integrantes de los grupos técnicos;
2. Proporcionar asesoría a los integrantes de los grupos técnicos;
3. Revisar la documentación generada en las actividades en materia de Seguridad de la Información y retroalimentar a los grupos técnicos, y
4. Las demás que establezcan las presentes Políticas, Lineamientos para el Fortalecimiento de la Seguridad de la Información en los Procesos y Servicios Institucionales y demás disposiciones administrativas aplicables.

Los datos de estos facilitadores serán notificados y, en su caso, actualizados mediante oficio al Presidente del Comité, en el que se incluirán nombre, cargo, ubicación física, número telefónico y cuenta de correo electrónico oficiales.

#### **I. Responsabilidades y Sanciones;**

Resultarán aplicables respecto de lo dispuesto en las presentes Políticas las sanciones establecidas en la Ley del Sistema Nacional de Información Estadística y Geográfica y la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos, sin perjuicio de las demás acciones legales y administrativas a que hubiere lugar para el Instituto, en cada caso.



## VI. INTERPRETACIÓN.-

La interpretación de las presentes Políticas de la Seguridad de la Información del Instituto Nacional de Estadística y Geografía, para efectos administrativos, corresponderá a la Dirección General de Integración, Análisis e Investigación quien propondrá la actualización de las mismas ante la instancia encargada de su aprobación. La solución de los casos no previstos por las Políticas corresponderá al Comité.

### TRANSITORIOS.

**PRIMERO.-** Las presentes Políticas entrarán en vigor al día hábil siguiente de su publicación en la Normateca Interna del Instituto.

**SEGUNDO.-** El Comité a que hace referencia la Sección I, numeral 5 de las presentes Políticas, deberá conformarse y emitir dentro de un plazo de 90 días hábiles posteriores a la entrada en vigor de las presentes Políticas, su Manual de Integración y Funcionamiento.

**TERCERO.-** El Comité deberá emitir dentro de un plazo de 90 días hábiles posteriores a su integración, la Estrategia General de Seguridad de la Información, Lineamientos para el Fortalecimiento de la Seguridad de la Información en los Procesos y Servicios Institucionales, El Protocolo Institucional de Respuesta a incidentes de Seguridad de la Información y Programa Anual de Trabajo del Comité del Sistema de Seguridad de la Información citados en las presentes Políticas.

Las presentes Políticas, se aprobaron en términos del Acuerdo No. 11<sup>a</sup>/XIII/2014, de la décimo primera sesión de la Junta de Gobierno del Instituto Nacional de Estadística y Geografía, celebrada el nueve de diciembre de 2014.- Presidente: Eduardo Sojo Garza Aldape.- Vicepresidentes: Enrique de Alba Guerra, Mario Palma Rojo, Rolando Ocampo Alcántar y Félix Vélez Fernández Varela.-Rubricas