POLÍTICA PARA LA SEGURIDAD DE LA INFORMACIÓN ESTADÍSTICA Y GEOGRÁFICA DEL INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA.

DIRECCIÓN GENERAL DE INTEGRACIÓN, ANÁLISIS E INVESTIGACIÓN.

Noviembre, 2020.
Aguascalientes, Aguascalientes.

ÍNDICE:

INTRODUCCIÓN.

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

La presente Política plantea las directrices para administrar los riesgos en materia de Seguridad de la información, de manera que cada Unidad Administrativa productora y transversal del Instituto establezca controles transversales para preservar la Seguridad de la información.

La Política tiene el propósito de establecer un marco de referencia general para delinear las directrices que las personas servidores públicos adscritos a las Unidades Administrativas productoras y transversales deben seguir para preservar la Confidencialidad, Integridad y Disponibilidad por medio de un esquema alineado con el proceso de producción regulado en la Norma Técnica del Proceso de Producción de Información Estadística y Geográfica para el Instituto Nacional de Estadística y Geografía, de tal forma que se contribuya a la consolidación del ecosistema de datos.

La Política debe interpretarse en el contexto del marco general de la normatividad en materia de Seguridad de la información del Instituto, de tal manera que su cumplimiento facilite la implementación de los Controles de seguridad de la información de forma inherente en el proceso de producción de Información.

Con el fin de establecer y definir las pautas de operación 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 la siguiente:

POLÍTICA PARA LA SEGURIDAD DE LA INFORMACIÓN ESTADÍSTICA Y GEOGRÁFICA DEL INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA

I. GLOSARIO.-

Para efectos de la presente Política 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, Integridad y Disponibilidad acorde al valor que se le otorgue;
2. **Activo de información crítico:** El Activo de información con una calificación de nivel alto en su Confidencialidad, Integridad o Disponibilidad;
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. **Actor del Rol Responsable del Proceso:** Persona servidor público designada por las personas titulares de las Unidades Administrativas en términos del artículo 7 de la Norma Técnica;
5. **Actor del Rol Responsable de la Fase:** Persona servidor público designada por el Actor del Rol Responsable del Proceso en términos del segundo párrafo del artículo 7 de la Norma Técnica;
6. **Área Contratante:** La facultada en la Unidad Administrativa para realizar procedimientos de contratación, a efecto de adquirir o arrendar bienes o contratar la prestación de servicios que el Instituto Nacional de Estadística y Geografía requiera;

7. **Área de acceso restringido:** Espacio físico al que sólo tiene acceso personal autorizado dado que contienen Activos de información con identificadores, datos individualizados de los Informantes u otro tipo de Información de divulgación definida como de acceso restringido, así como los centros de datos y áreas que contengan infraestructura tecnológica y de comunicaciones que sea considerada como crítica por la Coordinacion General de Informática;
8. **Área Requirente:** La que en la Unidad Administrativa solicite o requiera formalmente la adquisición o arrendamiento de bienes o la contratación de servicios, o bien, aquélla que los utilizará;
9. **Área Técnica:** La que en la Unidad Administrativa elabora las especificaciones técnicas, así como determina las normas de carácter técnico aplicables que se deberán incluir en el procedimiento de contratación; evalúa la propuesta técnica de las proposiciones, y es responsable de responder en la junta de aclaraciones, las preguntas que sobre estos aspectos realicen los licitantes;
10. **CGI:** Coordinación General de Informática;
11. **Comité:** El Comité de Seguridad y Confidencialidad Estadística de la Información;
12. **Compromiso de confidencialidad:** Documento firmado por las personas servidores públicos adscritas a las Unidades Administrativas productoras y transversales, mediante el cual ratifican y reiteran el conocimiento de las obligaciones a su cargo, en términos del marco normativo aplicable, respecto de las actividades mencionadas;
13. **Confidencialidad:** Atributo de Seguridad de la información que indica que la información sólo es revelada a individuos o procesos autorizados;
14. **Confidencialidad estadística:** Protección de los datos proporcionados por los Informantes del Sistema y, en general, de las personas físicas o morales objeto de la información, para evitar su Identificación directa o indirecta, así como su uso para fines no estadísticos, de conformidad con el artículo 47 de la Ley del SNIEG;

15. **Control de seguridad:** Medidas, procedimientos o acciones tendientes a administrar los riesgos en materia de Seguridad de la información para disminuir la probabilidad de su materialización y el impacto de éstos;
16. **DGAANAR:** Dirección General Adjunta de Apoyo Normativo y Administración de Riesgos;
17. **DGIAI:** Dirección General de Integración, Análisis e Investigación;
18. **Disponibilidad:** Atributo de Seguridad de la información que consiste en que la información permanece accesible para su uso cuando así lo requieran las personas servidores públicos o procesos autorizados;
19. **Enlace Informático:** La persona en una Unidad Administrativa responsable de apoyar y acordar con la CGI lo relacionado con la coordinación de la Función Informática al interior de la Unidad Administrativa de su adscripción;
20. **Enlace de Seguridad de la información:** La persona servidor público en la Junta de Gobierno y Presidencia, Coordinaciones Generales, Direcciones Generales Adjuntas, Direcciones Regionales y Coordinaciones Estatales responsable de apoyar al Vocal de su adscripción en la coordinación de las actividades en materia de Seguridad de la información y Confidencialidad estadística;
21. **Evento de seguridad de la información o Evento:** Circunstancia que indica una posible afectación a la Seguridad de la información;
22. **Incidente de seguridad de la información o Incidente:** Afectación en la Confidencialidad, Integridad o Disponibilidad de los Activos de información o de los Activos de TIC;
23. **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 SNIEG;
24. **Informantes del Sistema:** Personas físicas o morales, a quienes les sean solicitados datos estadísticos y geográficos;
25. **Instituto:** Instituto Nacional de Estadística y Geografía;
26. **Integridad:** Atributo de Seguridad de la información referente a que la información está completa y sin alteraciones;

27. **Norma Técnica:** Norma Técnica del Proceso de Producción de Información Estadística y Geográfica para el Instituto Nacional de Estadística y Geografía;
28. **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;
29. **Política:** Política para la Seguridad de la Información Estadística y Geográfica del Instituto Nacional de Estadística y Geografía;
30. **Prestadores de servicios:** Personal de empresas proveedoras de servicios que realizan labores en el interior del Instituto;
31. **Proceso:** Conjunto de actividades que interactúan entre sí, las cuales transforman elementos de entrada en resultados;
32. **Programa de Información o Programa:** Conjunto de actividades, que se pueden repetir, que describen el propósito y contexto de un conjunto de Procesos que se llevarán a cabo cada período de tiempo para producir información;
33. **Proveedor:** La persona que celebre contratos de adquisiciones, arrendamientos o servicios con el Instituto;
34. **Reglamento:** Reglamento Interior del Instituto Nacional de Estadística y Geografía;
35. **Repositorio de información:** Sistema electrónico de almacenamiento de información;
36. **Riesgo de seguridad de la información:** La probabilidad de que una amenaza pueda explotar una vulnerabilidad y causar pérdida o daño en la Confidencialidad, Integridad o Disponibilidad de los Activos de información del Instituto;
37. **Seguridad de la información:** Capacidad de preservar la Confidencialidad, Integridad y Disponibilidad de la información;
38. **Tecnologías de la Información y Comunicaciones o TIC:** Conjunto integrado por la Infraestructura Tecnológica, así como por los procedimientos y técnicas para procesar, acceder, almacenar, convertir, proteger, recuperar y transmitir Información Electrónica;

39. **Unidades Administrativas:** La Junta de Gobierno y Presidencia, las Direcciones Generales, las Coordinaciones Generales y las Direcciones Regionales;
40. **Unidades Administrativas productoras**: Las Unidades Administrativas que tienen a su cargo algún Programa de Información;
41. **Unidades Administrativas transversales**: Las Unidades Administrativas que, sin ser responsables de un Programa de Información, desarrollan actividades de administración de la información estadística y geográfica.

II. OBJETO.-

Establecer los principios generales para la gestión de la Seguridad de la información de la información estadística y geográfica para prevenir y disminuir el impacto de eventos adversos, que potencialmente podrían afectar el logro de los objetivos del Instituto.

III. ÁMBITO DE APLICACIÓN.-

La presente Política es de observancia general y obligatoria para las Unidades Administrativas productoras y transversales, así como para las personas servidores públicos adscritos a las mismas.

IV. 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 General de Archivos;
b.4. Ley de la Propiedad Industrial, y
b.5. Ley General de Responsabilidades Administrativas.

c) Reglamentos.

c.1. Reglamento de la Ley de la Propiedad Industrial;

c.2. Reglamento de la Ley Federal del Derecho de Autor, y

c.3. Reglamento Interior del Instituto Nacional de Estadística y Geografía.

d) Normas.

d.1. Norma para la difusión y promoción del acceso, conocimiento y uso de la Información Estadística y Geográfica que genera el Instituto Nacional de Estadística y Geografía;

d.2. Normas de Control Interno para el Instituto Nacional de Estadística y Geografía;

d.3. Norma Técnica del Proceso de Producción de Información Estadística y Geográfica para el Instituto Nacional de Estadística y Geografía;

d.4. Norma para el aseguramiento de la calidad de la información Estadística y Geográfica del Instituto Nacional de Estadística y Geografía, y

d.5. Normas en materia de Adquisiciones, Arrendamientos y Servicios del Instituto Nacional de Estadística y Geografía.

e) Políticas.

e.1. Políticas en materia de Tecnologías de la Información y Comunicaciones del Instituto Nacional de Estadística y Geografía;

e.2. Políticas para el Desarrollo de Sistemas Informáticos;

e.3. Políticas para la Continuidad de las Operaciones del Instituto Nacional de Estadística y Geografía;

e.4. Políticas para la Administración y uso de los Servicios Tecnológicos, y

e.5. Políticas para la Seguridad Informática.

f) Reglas.

f.1. Reglas de Operación del Laboratorio de Microdatos 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 del Proceso de Gestión de Cambios en los Programas de Información Estadística y Geográfica;

g.3. Lineamientos en Materia de Tecnologías de la Información y Comunicaciones del Instituto Nacional de Estadística y Geografía;

g.4. Lineamientos para el uso y portación de la credencial de identificación del Instituto Nacional de Estadística y Geografía;

g.5. Lineamientos para la Elaboración de Acta Entrega-Recepción que Observarán los Servidores Públicos del Instituto Nacional de Estadística y Geografía al Separarse de su Empleo, Cargo o Comisión;

g.6. Lineamientos para la organización y conservación de los archivos del Instituto Nacional de Estadística y Geografía;

g.7. Lineamientos para presentar información sobre la administración de riesgos, y

g.8. Lineamientos para el desarrollo y publicación de productos del INEGI.

V. POLÍTICAS GENERALES.-

Organización de la Seguridad de la información

Primera.- La gestión de la Seguridad de la información en el Instituto se concibe como la capacidad para preservar la Confidencialidad, Integridad y Disponibilidad de la Información con el objetivo de coadyuvar al cumplimiento de los objetivos institucionales.

Segunda.- Los aspectos particulares de Seguridad de la Información serán normados por las personas titulares de las Unidades Administrativas que correspondan según sus

atribuciones en el Reglamento. Los aspectos generales de Seguridad de la información serán normados por el Comité.

Tercera.- La gestión de la Seguridad de la información en el Instituto está organizada de la siguiente forma:

a) **Responsable de Seguridad de la información:** La persona servidor público titular de la Dirección General de Integración, Análisis e Investigación, conforme a lo establecido en el Reglamento, tiene la función de coordinar las acciones de Seguridad de la información, aprobar la estrategia en la materia y los documentos auxiliares que faciliten la instrumentación de las disposiciones normativas, como guías, plantillas e instructivos, y determinar las aplicaciones informáticas que se utilizará para sistematizar la gestión de la Seguridad de la información;

b) **Comité de Seguridad y Confidencialidad Estadística de la Información:** El órgano colegiado cuyo objetivo es contribuir al fortalecimiento de la Seguridad y Confidencialidad Estadística de la Información en el Instituto;

c) **La persona servidor público titular de la Dirección General Adjunta de Recursos Humanos:** conforme a lo establecido en el Reglamento, tiene la función de organizar e implementar políticas y procedimientos relacionados con el reclutamiento, selección, ingreso, evaluación, desarrollo profesional y separación del personal del Instituto;

d) **La persona servidor público titular de la Dirección General Adjunta de Recursos Materiales y Servicios Generales:** conforme a lo establecido en el Reglamento, tiene las funciones de coordinar la administración de bienes muebles e inmuebles; coordinar las acciones en materia de organización y conservación de archivos, y coordinar los sistemas de protección civil y de manejo ambiental;

e) **La persona servidor público titular de la DGAANAR:** conforme a lo establecido en el Reglamento, tiene las funciones de promover, coordinar y asesorar la implantación y mejora continua del control interno institucional; promover la cultura

de administración de riesgos y asesorar a las Unidades Administrativas del Instituto en la identificación de riesgos que afecten al logro de sus objetivos;

f) **La persona servidor público titular de la Coordinación General de Asuntos Jurídicos:** conforme a lo establecido en el Reglamento, tiene las funciones de coordinar la atención de los asuntos jurídicos del Instituto; revisar los requisitos legales a que deban sujetarse los convenios y contratos que deban suscribir las Unidades Administrativas, y representar jurídicamente al Instituto y gestionar los asuntos relacionados con la propiedad industrial y los derechos de autor, ante las autoridades competentes;

g) **La persona servidor público titular de la CGI:** conforme a lo establecido en el Reglamento, tiene las funciones siguientes: coordinar y determinar la organización de las áreas informáticas del Instituto, en coordinación con la Dirección General Adjunta de Recursos Humanos; proponer, instrumentar y dar seguimiento al cumplimiento de disposiciones normativas internas y criterios técnicos en materia de TIC; coordinar, diseñar, implementar y prestar a las Unidades Administrativas del Instituto los servicios de gestión de las TIC, de software, de cómputo y comunicaciones, de seguridad informática, de desarrollo de sistemas informáticos, de bases de datos y Repositorios de información electrónica, de soporte técnico, y de provisión de bienes y servicios informáticos; diseñar, establecer, coordinar y supervisar de manera continua el Sistema Integral de Seguridad Informática y de Comunicaciones del Instituto; coordinar el diseño, instrumentación, administración y operación de las plataformas de infraestructura de cómputo y comunicaciones, de servicios informáticos, de sistemas informáticos, de información electrónica, el Sistema Integral de Seguridad Informática y de Comunicaciones;

h) **La persona servidor público titular de la Dirección General de Comunicación, Servicio Público de Información y Relaciones Institucionales:** conforme a lo establecido en el Reglamento, tiene las funciones de dirigir y coordinar la prestación del Servicio Público de Información, así como la difusión de la información estadística y geográfica que genera e integra el

Instituto; dirigir y coordinar la estrategia de difusión de la información estadística y geográfica a través de Internet, y proponer las disposiciones normativas en materia del Servicio Público de Información, datos abiertos, atención a usuarios, detección de necesidades de información, difusión, vinculación institucional, comunicación, identidad institucional y de promoción de la información estadística y geográfica que genera e integra el Instituto y supervisar su aplicación;

i) **Grupo de Respuesta a Incidentes de seguridad de la información:** Su objetivo es analizar y proponer acciones para atender los Incidentes en la materia. Conformado por las personas servidores públicos con nivel jerárquico de Subdirección y Jefatura de Departamento adscritas a la Dirección de Seguridad y Confidencialidad de la Información y las personas servidores públicos designados por la DGAANAR y la CGI para colaborar en el análisis y atención de los Incidentes;

j) **Enlace de Seguridad de la información. En la Junta de Gobierno, Presidencia, y en las Coordinaciones Generales:** Es la persona servidor público, con puesto mínimo de Director de Área, designada por el titular de éstas para desempeñar dicha función. En las Direcciones Generales comprendidas entre las Unidades Administrativas productoras y transversales, es la persona servidor público, con puesto mínimo de Director de Área, designada en cada Dirección General Adjunta por el titular de éstas para desempeñar dicha función. En las Direcciones Regionales y Coordinaciones Estatales es la persona servidor público que realiza a nivel de Dirección y Subdirección de Área, respectivamente, la función de estadística. Tiene las funciones siguientes: colaborar con el Vocal de la Unidad Administrativa en la gestión de la Seguridad de la información, otorgar asesoría en las actividades de identificación de Activos de información, Áreas de acceso restringido y los requerimientos de redundancia tecnológica, dar seguimiento a la atención de los Eventos e Incidentes de Seguridad de la información, e informar al titular de la Unidad Administrativa del estado de Seguridad de la información;

k) **Responsable del activo de información:** En el ámbito de las Unidades Administrativas productoras es la persona servidor público designado por el Actor del Rol Responsable de la Fase. En el ámbito de las Unidades Administrativas transversales es la persona servidor público designado por cada titular de Dirección de Área en su ámbito de competencia. Tiene las funciones siguientes: coordinar la identificación y calificación de los Activos de información, verificar que se incluyan los riesgos asociados a la pérdida de la Confidencialidad, Integridad y Disponibilidad de los Activos de información críticos en la Matriz de Administración de Riesgos del Proceso, aprobar y verificar la implementación de los Controles de seguridad de información aplicables a los Activos de información, designar al Custodio de los activos de información, autorizar los permisos de acceso, lectura, escritura y eliminación en cada Activo de información, y documentar la aplicación de los Controles de seguridad de la información;

l) **Custodio del activo de información:** La persona servidor público designado por el Responsable del activo de información. En el caso de los Activos de información almacenados en la infraestructura de cómputo administrada por la CGI, es la persona servidor público a cargo de la administración tecnológica de éstos. Tiene las funciones siguientes: administrar y hacer efectivos los Controles de seguridad que el Responsable del activo de información haya definido en relación con el Activo de información;

m) **Responsable de Área de Acceso Restringido:** En el ámbito de las Unidades Administrativas productoras es la persona servidor público designado por el Actor del Rol Responsable de la Fase. En el ámbito de las Unidades Administrativas transversales es la persona servidor público designado por cada titular de Dirección de Área en su ámbito de competencia. Tiene las funciones siguientes: aprobar y verificar la implementación de los Controles de seguridad de información aplicables a las Áreas de acceso restringido;

n) **Enlace Informático:** Tiene como objetivo coadyuvar con el Vocal correspondiente a la Unidad Administrativa de su adscripción en el desempeño de sus funciones.

Cuarta.- El Comité se integrará de la siguiente forma:

a) **Presidente:** La persona servidor público titular de la Dirección General de Integración, Análisis e Investigación;

b) **Secretario Ejecutivo:** La persona servidor público titular de la Dirección General Adjunta de Integración de Información;

c) **Vocales:** Un representante de la Junta de Gobierno y Presidencia, las Direcciones Generales y las Coordinaciones Generales de Informática y de Operación Regional. En el caso de la Junta de Gobierno y Presidencia y las Coordinaciones Generales la persona servidor público designada debe tener nivel jerárquico de Dirección de Área. En el caso de las Direcciones Generales la persona servidor público designada debe tener nivel jerárquico de Dirección General Adjunta. Lo anterior con el fin de cubrir la visión integral de las implicaciones en la Seguridad y Confidencialidad estadística de la Información;

d) **Asesores:** Un representante del Órgano Interno de Control, de la Coordinación General de Asuntos Jurídicos, de las Direcciones Generales Adjuntas de: Recursos Materiales y Servicios Generales, y Recursos Humanos. Deben tener nivel jerárquico mínimo de Dirección de Área, e

e) **Invitados:** Las personas servidores públicos necesarios para el desahogo de los asuntos a tratar.

Quinta.- La gestión de Incidentes que afectan a la Información en su Confidencialidad, Integridad o Disponibilidad se atenderán conforme a la distribución siguiente:

a) **Incidentes de seguridad informática:** La atención de los eventos e incidentes relacionados con la afectación de los servicios de TIC se realizará conforme lo establezca la CGI. La CGI informará a la DGIAI y a la DGAANAR de los eventos e incidentes de seguridad informática que pongan en riesgo la Confidencialidad, Integridad y Disponibilidad de los Activos de información, así como la continuidad

del proceso de producción de Información con el fin de coordinarse para su atención.

b) **Incidentes de seguridad de la información:** La atención de los Eventos e Incidentes relacionados con la afectación de la Confidencialidad, Integridad y Disponibilidad de los Activos de información o soportados en Activos de TIC pertenecientes a las Unidades Administrativas productoras y transversales se realizará conforme lo establezca el Comité.

Sexta.- El Grupo de Respuesta a Incidentes de Seguridad de la información tendrá la responsabilidad de coordinar el análisis de las notificaciones de Eventos de seguridad de la información considerando lo definido en la normatividad aplicable en la materia.

Séptima.- La Información generada en el Instituto pertenece a éste, a menos que mediante un instrumento jurídico 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 autorizar el acceso a los Activos de información corresponde al Responsable del activo de información.

Gestión de la Seguridad de la información

Octava.- La persona titular de la DGIAI como Responsable de la Seguridad de la información deberá coordinar:

a) La revisión de la presente Política al menos una vez al año para determinar la necesidad de su actualización, tomando en consideración los cambios en la legislación aplicable, los informes de las revisiones internas y externas, los avances tecnológicos y los requerimientos propios del INEGI para el cumplimiento de sus objetivos;

b) El contacto con las autoridades pertinentes respecto de la atención de Incidentes de seguridad de la información que lo demanden;

c) El contacto con grupos de interés que le permitan mejorar el conocimiento en la materia;

d) Las acciones de concientización en materia de Seguridad de la información para las personas servidores públicos adscritas a las Unidades Administrativas productoras y transversales del Instituto, y

e) Las acciones de capacitación en temas de aplicación general en la materia para las personas servidores públicos adscritas a las Unidades Administrativas productoras y transversales del Instituto.

Novena.- Son funciones del Comité:

a) Coordinar la revisión y aprobación por parte de las Unidades Administrativas productoras y transversales del Inventario de Activos de información, el Inventario de Áreas de acceso restringido y el Inventario de Requerimientos de Redundancia Tecnológica;

b) Coordinar la revisión de la aplicación de los Controles de seguridad en los Activos de información críticos por lo menos una vez al año, y

c) Gestionar la realización de revisiones externas en materia de Seguridad de la Información para identificar la efectividad de los Controles establecidos para proteger la Información. Los resultados de las revisiones deben tomarse en cuenta para la implementación de mejoras;

d) Emitir las disposiciones normativas y administrativas tendientes a fortalecer la coordinación de la Seguridad de la información en el Instituto;

e) Elaborar y aprobar el Manual de Integración, así como sus actualizaciones subsecuentes;

f) Aprobar el acta de cada sesión a más tardar en la sesión ordinaria inmediata posterior a su celebración;

g) Aprobar el informe anual respecto de los resultados obtenidos de su actuación, en la primera sesión ordinaria del ejercicio fiscal inmediato posterior;

h) Aprobar la creación de grupos de trabajo que coadyuven al cumplimiento del

Programa de Trabajo del Comité, determinando la materia de competencia de cada uno, las Áreas y los niveles jerárquicos de las personas servidores públicos que los integran, así como la forma y términos en que deberán informar al Comité de los asuntos que conozcan;

i) Aprobar, en la última sesión de cada ejercicio fiscal, el calendario anual de sesiones ordinarias y el Programa Anual de Trabajo del Comité, del año siguiente, y

j) Vigilar el cumplimiento de los Acuerdos que se generen en el Comité, así como el seguimiento de los mismos.

Décima.- Las personas titulares de las Unidades Administrativas productoras y transversales, en el ámbito de su competencia, deberán proporcionar las facilidades para que el personal participe en los eventos de capacitación y concientización promovidos por el Responsable de Seguridad de la información.

Décima Primera.- El Enlace de Seguridad de la información, en el ámbito de su competencia, deberá:

a) Coordinar que el Inventario de Activos de información, el Inventario de Áreas de acceso restringido y el Inventario de Requerimientos de Redundancia Tecnológica se mantengan actualizados;

b) Revisar que los datos contenidos en el Inventario de Activos de información, el Inventario de Áreas de acceso restringido y el Inventario de Requerimientos de Redundancia Tecnológica corresponda con la totalidad de los Programas de Información a cargo de la Unidad Administrativa productora y con el desarrollo de las funciones correspondientes a las Unidades Administrativas transversales;

c) Coordinarse con el Enlace Informático para entregar a la CGI los requerimientos de redundancia tecnológica, y

d) Identificar las necesidades de capacitación específicas en materia de Seguridad de la información de la Unidad Administrativa para su gestión ante la Dirección de Capacitación.

Décima Segunda.- En las Unidades Administrativas transversales corresponde a las personas servidores públicos con puesto de Dirección de Área, en el ámbito de su competencia, coordinar y verificar el cumplimiento de las políticas Décima Tercera y Décima Cuarta.

Décima Tercera.- El Actor del Rol Responsable del Proceso con el apoyo del Actor del Rol Responsable de la Fase de Diseño, coordinará, al menos una vez al año, la revisión y actualización de los Riesgos de seguridad de la información y los Controles correspondientes a los Activos de información críticos con el fin de asegurarse de que estos son efectivos para preservar la Confidencialidad, Integridad y Disponibilidad de la Información.

Décima Cuarta.- El Actor del Rol de Responsable de la Fase deberá:

a) Definir e implementar mecanismos para que las personas servidores públicos y Personal externo que tengan acceso a la Información conozcan sus responsabilidades en materia de Seguridad de la información, así como de los controles que deben aplicar para preservar la Confidencialidad, Integridad y Disponibilidad de ésta;

b) Definir e implementar mecanismos para asegurar que cada persona servidor público:

i. Al asumir su cargo o comisión reciba de manera explícita la lista de los Activos de información en los que fungirá como Responsable y en su caso Custodio, y

ii. Al concluir su relación laboral o cuando cambien sus funciones entregue los Activos de información de los que fungía como Responsable y, en su

caso, Custodio, y se le revoquen los permisos para ingresar a las Áreas de acceso restringido, a los Repositorios de información y a los aplicativos informáticos que le fueron asignados por motivo de sus funciones;

c) Designar al Responsable de cada Activo de información y al Responsable de área de acceso restringido;

d) Revisar periódicamente que el manejo de los Activos de información y los procedimientos dentro de su ámbito de competencia cumplen con lo establecido en la presente política y con el resto de la normatividad aplicable en la materia, así como de implementar acciones correctivas ante un incumplimiento;

e) Asegurarse de que el manejo de los Activos de información se realiza conforme su calificación a lo largo de todo su ciclo de vida, conforme a las disposiciones aplicables en la materia;

f) Reportar ante las autoridades competentes conforme a la normatividad que corresponda el incumplimiento de la normatividad en materia de Seguridad de la información por parte de las personas servidores públicos del Instituto y del Personal externo;

g) Reportar las situaciones que puedan representar un Riesgo de seguridad de la información y la materialización de éstos a través del servicio de Mesa de Ayuda institucional;

h) Definir los Controles de seguridad de la información para los Activos de información críticos en los planes y acciones que se elaboren para mantener la continuidad del proceso y de recuperación de desastres, y

i) Coordinar la identificación de Áreas de acceso restringido y la implementación de Controles de seguridad para regular el acceso a éstas.

Décima Quinta.- Las personas servidores públicos Responsables de los Activos de información deberán:

a) Asegurar que los Activos de información son inventariados, calificados y en su caso vueltos a calificar conforme a las necesidades de protección de Confidencialidad, Integridad y Disponibilidad de la Información;

b) Asegurar que en los metadatos de los Activos de información se incluyen los datos referentes a su calificación, conforme a la normatividad correspondiente en la materia, y

c) Aplicar o solicitar la aplicación de los Controles de seguridad conforme a la calificación de los Activos de información.

Décima Sexta.- El Área Requirente de manera conjunta con el Área Técnica establecerán los requisitos que en materia de Seguridad de la información deben cumplir los proveedores que tengan acceso a los Activos de información que contengan identificadores, datos individuales de los Informantes u otro tipo de Información de divulgación restringida. El Área Contratante documentará los requisitos y los registrará en el contrato correspondiente, entre otros:

a) Que la Información a la que el Proveedor tiene acceso y conoce, por omisión, es confidencial y no podrá ser utilizada en ningún caso fuera de lo establecido en el correspondiente contrato;

b) El uso adecuado de los recursos del Instituto, especialmente en lo referido a los controles de acceso físico y lógico, y

c) En su caso, los Controles que permitan tratar los Riesgos de seguridad de la información, asociados a la cadena de suministro de los servicios y productos de TIC.

Décima Séptima.- El Área Requirente verificará el cumplimiento de los requisitos de Seguridad de información respecto de la prestación de servicios del Proveedor.

Décima Octava.- Las personas servidores públicos adscritos a las Unidades Administrativas productoras y transversales deberán:

a) Firmar el Compromiso de confidencialidad cuando tomen el encargo. Las personas servidores públicos de confianza deberán renovar su firma de compromiso al menos cada seis años;

b) Utilizar los Activos de información institucionales exclusivamente para el desarrollo de sus funciones con el fin de preservar la Confidencialidad, Integridad y Disponibilidad de la Información, para lo cual deben atender lo establecido en la normatividad institucional;

c) Clasificar la documentación, independientemente del medio que la contenga, conforme a lo especificado en la legislación y normatividad administrativa vigentes en materia de archivos;

d) Entregar al Actor del Rol Responsable de la Fase los Activos de información de los cuales son responsables y custodios cuando ocurra un cambio de funciones o cese la relación laboral con el Instituto;

e) Reportar los Eventos de seguridad de la información por medio del servicio de Mesa de Ayuda institucional o de los mecanismos que el Comité defina para tal fin, y

f) Observar durante el desarrollo de su jornada laboral lo siguiente:

i. Al levantarse del puesto de trabajo y al finalizar la jornada laboral, los escritorios deben permanecer despejados y libres de documentos físicos y/o medios extraíbles que contengan identificadores, datos individuales de los Informantes u otro tipo de Información de divulgación restringida, estos deben guardarse en un lugar seguro y bajo llave;

ii. Cuando se impriman o digitalicen documentos que contengan identificadores, datos individuales de los Informantes u otro tipo de Información de divulgación restringida, estos deben retirarse inmediatamente de los dispositivos de impresión y digitalización;

iii. Los gabinetes, cajones y archivadores que contengan documentos y/o medios extraíbles con identificadores, datos individuales de los Informantes

u otro tipo de Información de divulgación restringida deben permanecer cerrados, con la excepción durante su uso en la jornada laboral, y

iv. Al levantarse del puesto de trabajo, se debe bloquear la sesión de los equipos de cómputo para proteger el acceso a las aplicaciones y servicios institucionales.

De la vinculación institucional en materia de Seguridad de la información

Décima Novena.- Corresponde a la Dirección General Adjunta de Recursos Humanos:

a) Coordinar las acciones para que todas las personas servidores públicos del Instituto adscritas a las Unidades Administrativas productoras y transversales:

i. Firmen el Compromiso de confidencialidad al momento de su contratación;

ii. Participen en las acciones de capacitación en materia de Seguridad y Confidencialidad estadística;

b) Informar anualmente al Comité, por medio del asesor, los resultados de las acciones de capacitación en materia de Seguridad y Confidencialidad estadística.

Vigésima.- Corresponde a la Dirección General Adjunta de Recursos Materiales y Servicios Generales:

a) Establecer los controles de acceso físico en las instalaciones del Instituto;

b) Generar y actualizar el Inventario de Bienes inmuebles del Instituto, el cual deberá entregar al Comité en enero de cada año y debe contener los datos siguientes: descripción, tipo de uso, ubicación, persona servidor público responsable, infraestructura de operación crítica (como subestaciones eléctricas y cuartos de máquinas) y nivel de criticidad para la operación del Instituto, y

c) Regular el control de acceso de las Áreas de acceso restringido.

Vigésima Primera.- Corresponde a la DGAANAR:

a) Regular la administración de riesgos, control interno y continuidad de las operaciones;

b) Informar, por medio del Vocal de la Dirección General de Administración, anualmente al Comité de:

i. Los riesgos principales que los Actores del Rol Responsable del Proceso hayan incorporado en materia de Seguridad y Confidencialidad estadística para los Programas de Información, y

ii. Los Procesos, Fases o Subprocesos Críticos y los Productos o Servicios Esenciales de los Programas de Información.

c) Colaborar con el Grupo de Respuesta a Incidentes de Seguridad de la información en el análisis y evaluación de los Incidentes de seguridad de la información a efecto de que no vuelvan a ocurrir;

Vigésima Segunda.- Corresponde a la CGI:

a) Entregar, en enero de cada año al Comité, por medio del Vocal el Inventario de la Infraestructura Crítica de TIC del Instituto y hacer de su conocimiento los resultados del análisis de riesgos, de vulnerabilidades y pruebas de penetración que le sean aplicados;

b) Colaborar con el Enlace de Seguridad de la información de las Unidades Administrativas correspondientes y con el apoyo de la DGAANAR en el análisis de los riesgos y la definición de los Controles de seguridad que permitan administrar los Riesgos asociados a los cambios en la Infraestructura tecnológica sobre la cual operan las actividades de las Unidades Administrativas productoras y transversales;

c) Informar, por medio del Vocal, en octubre de cada año al Comité de:

i. Los Controles implementados para cubrir los requerimientos de redundancia tecnológica de las Unidades Administrativas productoras y transversales, así como de los controles implementados para regular el acceso y proteger el perímetro de los centros de datos y otras áreas que

almacenen equipos de TIC que resulten fundamentales para el logro de los objetivos institucionales, y

ii. Los resultados de las pruebas técnicas que se apliquen, tanto por personal interno como externo, en la infraestructura tecnológica sobre la cual operan las actividades de las Unidades Administrativas productoras y transversales.

d) Implementar los Controles pertinentes para mantener la Confidencialidad, Integridad y Disponibilidad de la Información durante el desarrollo de las actividades de mantenimiento y reparación de los equipos e infraestructura de TIC;

e) Informar con la debida anticipación a los Actores del Rol Responsable del Proceso correspondientes sobre las fechas y horarios en los que se realizarán las actividades de mantenimiento y reparación de los equipos e infraestructura de TIC que pudieran poner en riesgo la Confidencialidad, Integridad y Disponibilidad de la Información;

f) Implementar los Controles pertinentes para conservar de forma segura las bitácoras relacionadas con el manejo de los Activos de información críticos, revisarlas de manera periódica e informar al Actor del Rol Responsable de la Fase de los Eventos detectados;

g) Definir las técnicas y mecanismos autorizados para realizar el cifrado de Información;

h) En su caso, implementar y operar el software de prevención de pérdida de datos;

i) Establecer los Controles pertinentes para que las pruebas de auditoría no afecten la Confidencialidad, Integridad y Disponibilidad de los sistemas de información tecnológica e informar al Comité y al Responsable de Proceso los resultados de dichas pruebas, y

j) Colaborar con el Grupo de Respuesta a Incidentes de Seguridad de la información, a través de la Dirección de Seguridad Informática, en el análisis, evaluación y respuesta de los Incidentes de Seguridad de la información.

VI. POLÍTICAS ESPECÍFICAS.-

a) De aplicación Transversal en el Proceso de Producción de Información

Vigésima Tercera.- El Enlace de Seguridad de la información promoverá, en el ámbito de su competencia, que en los Programas que se generen para producir Información sean analizados al menos una vez cada año, los riesgos asociados con la pérdida de la Confidencialidad, Integridad y Disponibilidad de la Información.

Vigésima Cuarta.- Le corresponde al Actor del Rol Responsable de la Fase, en su ámbito de competencia:

a) Verificar la implementación de los Controles correspondientes conforme se identificaron en la Fase de Diseño;

b) Solicitar a la CGI la inclusión del monitoreo automático de los Activos de información críticos a través del software de prevención de pérdida de datos con el que cuente el Instituto;

c) Integrar un informe sobre los Controles de seguridad de información implementados y los incidentes que afectaron la Confidencialidad, Integridad y Disponibilidad, el cual formará parte del reporte de evaluación referido en el artículo 35 de la Norma Técnica;

d) Asegurar que se aplican los Controles correspondientes para evitar la identificación de las personas físicas o morales objeto de la Información, así como evitar el uso para fines distintos al estadístico, de acuerdo con lo establecido en la Ley del SNIEG y en la normatividad aplicable en la materia;

e) Coordinar que previo a la salida de los Activos de información de las oficinas del Instituto se les apliquen los Controles para asegurar la Confidencialidad, Integridad y Disponibilidad de la Información;

f) Gestionar que, antes de su baja, donación, destrucción o reasignación, se apliquen procedimientos de borrado seguro en los equipos cómputo que que

contengan datos individuales proporcionados por los Informantes del Sistema, así como los que sean calificados como Activos de información críticos;

g) Gestionar la destrucción de los instrumentos impresos cuando ya no sean de utilidad para la producción de Información, de tal manera que no sea posible identificar los datos que contenían. Estas acciones deben realizarse en apego a lo establecido en la Ley General de Archivos y normatividad interna aplicable en lo que se refiere a la baja documental;

h) Definir, al menos una vez al año, los requerimientos de respaldos de los Activos de información, para la implementación y verificación de la Integridad de estos, para lo cual deberá coordinarse con el Enlace informático correspondiente, y

i) Definir los Repositorios de información y aplicativos en los que se requiere activar la generación de bitácoras con el fin de contar con elementos para detectar anomalías o cambios no deseados en los Activos de información críticos.

Vigésima Quinta.- Corresponde a la persona servidor público Responsable de los Activos de información:

a) Asegurarse de que la Información con identificadores contenida en los medios de almacenamiento extraíbles esté cifrada;

b) Previo a la baja, donación, destrucción o reasignación de los medios de almacenamiento extraíbles, gestionar con el Enlace Informático correspondiente que se realice el borrado seguro en medios de almacenamiento extraíbles que contengan identificadores, datos individuales de los Informantes u otro tipo de Información de divulgación restringida, y

c) Aplicar los Controles de protección a los medios extraíbles que contengan Información conforme se establece en las disposiciones institucionales en materia de TIC.

Vigésima Sexta.- Las personas servidores públicos adscritas a las Unidades Administrativas productoras:

a) Cuando utilicen equipos de cómputo móvil o se realicen actividades de trabajo fuera de oficina atenderán los controles que aseguren la Confidencialidad, Integridad y Disponibilidad de la Información, considerando para ello lo establecido en la normatividad institucional;

b) Deben abstenerse de depositar o enviar la Información a través de servicios que no forman parte de los servicios informáticos definidos para este fin en el proceso correspondiente o administrados por la CGI, y

c) Deben abstenerse de enviar por correo electrónico o por mensajería electrónica archivos que contengan identificadores, datos individuales u otro tipo de Información de divulgación restringida, con el fin de no comprometer la Confidencialidad de la Información.

Vigésima Séptima.- La Información que contenga identificadores, datos individuales de los Informantes u otro tipo de Información de divulgación restringida, deberá almacenarse y transmitirse de manera cifrada y utilizar canales de transmisión cifrados. El Actor del Rol Responsable de cada Fase establecerá las excepciones de cifrado en su ámbito de competencia.

b) De aplicación en la Fase de Documentación de las Necesidades

Vigésima Octava.- El Actor del Rol Responsable de la Fase en el desarrollo de las acciones para la detección, gestión y aprobación de necesidades deberá incluir en el Documento de detección de necesidades las disposiciones normativas en materia de Seguridad de la información en las que se establezcan obligaciones a cubrir.

c) De aplicación en la Fase de Diseño

Vigésima Novena.- El Actor del Rol Responsable de la Fase de Diseño:

a) Coordinará y colaborará con los Actores del Rol Responsable del resto de las Fases del proceso de producción, del Enlace de Seguridad de la información y del Enlace Informático correspondiente, la identificación de los riesgos que afecten la Confidencialidad, Integridad y Disponibilidad de la Información a lo largo de todo el proceso, así como de los controles necesarios para mitigarlos, e

b) Integrará los requerimientos de Confidencialidad, Integridad y Disponibilidad de la Información aplicables en todo el ciclo de vida de las plataformas informáticas, componentes, aplicaciones y servicios de software.

d) De aplicación en la Fase de Construcción

Trigésima.- El Actor del Rol de Responsable de la Fase de Construcción deberá:

a) Coordinar que, en la construcción y prueba de la infraestructura informática, los componentes, aplicaciones y servicios de software, se tomen en cuenta los requerimientos y Controles definidos en la Fase de Diseño, y

b) Asegurarse de que los datos que se utilizarán en las pruebas del desarrollo de los sistemas de información no contengan identificadores ni otro tipo de Información de divulgación restringida, con el fin de no comprometer la Confidencialidad de la Información. Los casos de excepción deberán documentarse.

e) De aplicación en la Fase de Captación

Trigésima Primera.- El Actor del Rol Responsable de la Fase de Captación deberá:

a) Coordinar la implementación de acciones para verificar que los procesos y tecnología cuentan con las condiciones de Seguridad necesarias para proteger la Información durante la captación de datos, independientemente del método a través del cual se realice, y

b) Coordinar que la capacitación que se dirija al personal que hará la captación de datos incluya temas para preservar la Confidencialidad, Integridad y Disponibilidad de la Información.

f) De aplicación en la Fase de Procesamiento

Trigésima Segunda.- El Actor del Rol Responsable de la Fase de Procesamiento deberá coordinar la implementación de Controles para preservar la Confidencialidad, Integridad y Disponibilidad de la Información en los procesos de transformación como clasificación, codificación, revisión, validación, edición e imputación de los mismos.

g) De aplicación en la Fase de Análisis de Producción

Trigésima Tercera.- El Actor del Rol Responsable de la Fase de Análisis de Producción deberá coordinar que en la realización de las actividades para producir resultados geográficos o estadísticos, se proteja la Confidencialidad, Integridad y Disponibilidad de la Información.

h) De aplicación en la Fase de Difusión

Trigésima Cuarta.- El Actor del Rol Responsable de la Fase de Difusión deberá coordinar la implementación de acciones para garantizar la Confidenciliad, Integridad y Disponibilidad de la Información.

i) De aplicación en la Fase de Evaluación del Proceso

Trigésima Quinta.- El Actor del Rol Responsable de la Fase de Evaluación del Proceso, en coordinación con los Actores del Rol Responsable de las otras Fases, deberá

incorporar los aspectos relacionados con la Seguridad y Confidencialidad estadística en el reporte de evaluación referido en el artículo 35 de la Norma Técnica.

j) De aplicación para las Unidades Administrativas transversales

Trigésima Sexta.- El Enlace de Seguridad de la Información de las Unidades Administrativas transversales coordinará la implementación de acciones para proteger la confidencialidad integridad y disponibilidad de la Información, conforme a lo que se establece en las siguientes políticas específicas.

Trigésima Séptima.- Las Unidades Administrativas transversales en la planeación de sus actividades, con el fin de preservar la Seguridad de la información, deberán observar lo siguiente:

- **a)** Identificar los riesgos que afecten la Confidencialidad, Integridad y Disponibilidad de los Activos de información de los que son responsables, así como los controles necesarios para administrarlos;
- **b)** Integrar las características para preservar la Confidencialidad, Integridad y Disponibilidad de la Información en los requerimientos del desarrollo de las plataformas, componentes, aplicaciones y servicios de software, aplicables en todo el ciclo de vida de éstos;
- **c)** Solicitar, a través del Enlace Informático, a la CGI la inclusión del monitoreo automático de los Activos de información críticos a través del software de prevención de pérdida de datos con el que cuente el Instituto;
- **d)** Definir, al menos una vez al año, los requerimientos de respaldos de los Activos de información, para la implementación y verificación de la Integridad de estos deberá coordinarse con el Enlace Informático correspondiente, y
- **e)** Asegurarse de que los datos que se utilizarán en las pruebas del desarrollo de los sistemas de información no contengan identificadores ni otro tipo de Información de

divulgación restringida, con el fin de no comprometer la Confidencialidad de la Información. Los casos de excepción deberán documentarse.

Trigésima Octava.- Las Unidades Administrativas transversales en la ejecución de sus actividades, con el fin de preservar la Seguridad de la información, deberán observar lo siguiente:

a) Verificar la implementación de los Controles de seguridad de información correspondientes conforme se identificaron en las acciones de planeación;

b) Coordinar que previo a la salida de los Activos de información de las oficinas del Instituto se les apliquen los Controles para asegurar la Confidencialidad, Integridad y Disponibilidad de la Información;

c) Gestionar que, antes de su baja, donación, destrucción o reasignación, se apliquen procedimientos de borrado seguro en los equipos cómputo que que contengan datos individuales proporcionados por los Informantes del Sistema, así como los que sean calificados como Activos de información críticos;

d) Aplicar los Controles de protección a los medios extraíbles que contengan Información conforme se establece en las disposiciones institucionales en materia de TIC;

e) Deben abstenerse de depositar o enviar la Información a través de servicios que no forman parte de los servicios informáticos definidos para este fin en el proceso correspondiente o administrados por la CGI, y

f) Deben abstenerse de enviar por correo electrónico o por mensajería electrónica archivos que contengan identificadores, datos individuales u otro tipo de Información de divulgación restringida, con el fin de no comprometer la Confidencialidad de la Información.

VII. INTERPRETACIÓN.-

La interpretación de la presente Política para la Seguridad de la Información Estadística y Geográfica 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 estas ante la instancia encargada de su aprobación. La solución de los casos no previstos por las Políticas corresponderá al Comité.

TRANSITORIOS.

PRIMERO.- La presente Política entrará en vigor al día hábil siguiente de su publicación en la Normateca Institucional.

SEGUNDO.- La presente Política deja sin efecto las Políticas para la Seguridad de la Información del Instituto Nacional de Estadística y Geografía, y las disposiciones que emitió el Comité del Sistema de Seguridad de la Información del Instituto Nacional de Estadística y Geografía.

TERCERO.- El Comité a que hace referencia la política Cuarta deberá conformarse y emitir su Manual de Integración y Funcionamiento dentro de un plazo de 30 días hábiles posteriores a la entrada en vigor de la presente Política.

CUARTO.- El Comité a que hace referencia la política Cuarta dará continuidad a las acciones de fortalecimiento de la Seguridad de la información estadística y geográfica definidas en el Programa Anual de Trabajo del Comité del Sistema de Seguridad de la Información.

QUINTO.- El Comité deberá emitir dentro de un plazo de 30 días hábiles posteriores a su integración, los Lineamientos para la Seguridad de la información estadística y geográfica del INEGI.

La presente Política, se aprobó en términos del Acuerdo No. 10ª/V/2020, de la Décima sesión de la Junta de Gobierno del Instituto Nacional de Estadística y Geografía, celebrada el 10 de noviembre de 2020.- Presidente: **Julio Alfonso Santaella Castell**, Vicepresidentes: **Enrique de Alba Guerra, Adrián Franco Barrios, Paloma Merodio Gómez** y **Enrique de Jesús Ordaz López**.

ÚLTIMA HOJA DE LA POLÍTICA PARA LA SEGURIDAD DE LA INFORMACIÓN ESTADÍSTICA Y GEOGRÁFICA DEL INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA, PUBLICADAS EN LA NORMATECA INSTITUCIONAL A LOS 26 DÍAS DEL MES DE NOVIEMBRE DE 2020, MISMAS QUE SE HACEN CONSTAR EN 34 DE FOJAS ÚTILES.

FE DE ERRATAS A LA POLÍTICA PARA LA SEGURIDAD DE LA INFORMACIÓN ESTADÍSTICA Y GEOGRÁFICA DEL INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA

Fe de erratas para la Normateca Institucional 14 de noviembre de 2022.

Página 24,

Dice:

Política Vigésima Segunda. - Corresponde a la CGI:…

b) Colaborar con el Enlace de Seguridad de la información de las Unidades Administrativas correspondientes y con el apoyo de la DGART…

Debe decir:

Política Vigésima Segunda. - Corresponde a la CGI:…

b) Colaborar con el Enlace de Seguridad de la información de las Unidades Administrativas correspondientes y con el apoyo de la DGAANAR…