LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN ESTADÍSTICA Y GEOGRÁFICA DEL INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA

COMITÉ DE SEGURIDAD Y CONFIDENCIALIDAD ESTADÍSTICA DE LA INFORMACIÓN

Abril, 2021
Aguascalientes, Aguascalientes.

ÍNDICE

INTRODUCCIÓN

El Instituto Nacional de Estadística y Geografía (Instituto) es un 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 para operar el Servicio Público de Información y otros productos y servicios que resultan importantes para la toma de decisiones en el país.

Los presentes Lineamientos se derivan de la Política para la Seguridad de la Información Estadística y Geográfica del Instituto Nacional de Estadística y Geografía con el objetivo de enfrentar de manera sistémica los riesgos en materia de Seguridad de la información, de manera que cada Unidad Administrativa productora y transversal instrumente los controles para preservar la Seguridad de la información estadística y geográfica.

Los Lineamientos plantean las directrices que deben seguir las personas servidores públicos que participan en el proceso de producción de información en la administración de la información para preservar la Confidencialidad, Integridad y Disponibilidad por medio de un esquema alineado a 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.

Los Lineamientos deben 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 manera inherente en el proceso de producción de información.

Por lo anterior, con fundamento en el numeral 6.3.1., inciso b), del Manual de Integración y Funcionamiento del Comité, este órgano colegiado tiene a bien emitir los siguientes:

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

CAPÍTULO I,
Lineamientos Generales

Artículo 1.- Los presentes Lineamientos tienen por objeto establecer las disposiciones a partir de las cuales las Unidades Administrativas productoras y transversales del Instituto, al amparo de su ámbito de competencia, instrumentarán los Controles para fortalecer la Seguridad de la información.

Artículo 2.- Los presentes Lineamientos son de observancia general y obligatoria para las Unidades Administrativas productoras y transversales, así como para las personas servidores públicos adscritas a las mismas.

Artículo 3.- Resultan aplicables los conceptos contenidos en el apartado I, denominado: Glosario de la Política para la Seguridad de la Información Estadística y Geográfica del Instituto Nacional de Estadística y Geografía, y en el artículo 3 de la Norma Técnica del Proceso de Producción de Información Estadística y Geográfica para el Instituto Nacional de Estadística y Geografía, así mismo para efectos de los presentes Lineamientos se entenderá por:

I. **Grupo de Respuesta a Incidentes de seguridad de la información:** Al grupo conformado por las personas servidores públicos con nivel jerárquico de subdirección y jefatura de departamento de la Dirección de Seguridad y Confidencialidad de la información, las personas servidores públicos designados por la Dirección General Adjunta de Apoyo Normativo y Administración de Riesgos (DGAANAR) y la Coordinación General de Informática (CGI), así como el Enlace de Seguridad de la información adscrito a la Unidad Administrativa en la que se presente el Incidente;

II. **Infraestructura de Información:** Conjunto de datos y metodologías que soportan el proceso de producción de información, así como su interacción e integración. Se compone de Catálogos y Clasificaciones; Registros Estadísticos y Geográficos, así como de Metodologías;

III. **Lineamientos:** Lineamientos de Seguridad de la Información Estadística y Geográfica del Instituto Nacional de Estadística y Geografía;

IV. **Política:** Política para la Seguridad de la Información Estadística y Geográfica del Instituto Nacional de Estadística y Geografía;

V. **Procesos, Fases o Subprocesos Críticos:** Conjunto de actividades, recursos humanos, datos e infraestructura relacionados lógicamente para producir un resultado que, de no obtenerse, pondría en riesgo la entrega de un producto o servicio esencial;

VI. **Productos o Servicios Esenciales:** Son vitales para el cumplimiento de la misión del Instituto y, como resultado final de un proceso, se ponen a disposición de los usuarios finales;

VII. **Redundancia tecnológica:** Característica de algunos sistemas en los que repiten aquellos datos, hardware o servicios de carácter crítico que son necesarios para asegurar la continuidad ante posibles fallos;

VIII. **Respaldo:** Copia de datos que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida;

IX. **Teletrabajo:** Forma de organizar y realizar el trabajo a distancia mediante la utilización de las TIC en el domicilio de la persona servidor público o en lugares o establecimientos ajenos al Instituto, y

X. **Unidades Administrativas:** La Junta de Gobierno y Presidencia, las Direcciones Generales, las Coordinaciones Generales y las Direcciones Regionales del Instituto Nacional de Estadística y Geografía.

Artículo 4.- Las Unidades Administrativas productoras y transversales, así como las Direcciones Regionales deberán integrar y actualizar en el primer trimestre de cada año, en el ámbito de su competencia, por medio de la aplicación informática determinada por la DGIAI para tal fin, el Inventario de Activos de información y el Inventario de Áreas de acceso restringido. Las personas titulares de las Unidades Administrativas productoras y transversales notificarán la actualización y aprobación de los inventarios mediante oficio al Secretario Ejecutivo del Comité, a más tardar dentro de los primeros cinco días hábiles del mes de abril.

Artículo 5.- Las Unidades Administrativas productoras y transversales, deberán integrar y actualizar en el primer trimestre de cada año, en el ámbito de su competencia, por medio de la aplicación informática determinada por la DGIAI para tal fin, el Inventario de Requerimientos de Redundancia tecnológica. Las personas titulares de las Unidades Administrativas productoras y transversales notificarán la actualización y aprobación del inventario mediante oficio al Secretario Ejecutivo del Comité, a más tardar dentro de los primeros cinco días hábiles del mes de abril.

CAPÍTULO II,
De la Integración de Inventarios para la Seguridad de la información

Sección I,
Inventario de Activos de información.

Artículo 6.- El Catálogo de Activos de información será de aplicación general y obligatoria para los Responsables de los Activos de información, con la finalidad de identificar los Activos de información con base en lo siguiente:

I. **Base de datos:** Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso;

II. **Sistemas Informáticos:** Conjunto de algoritmos y procedimientos que conforman aplicaciones o programas de cómputo que permiten procesar y almacenar datos bajo requerimientos definidos para cubrir alguna necesidad específica;

III. **Colecciones de imágenes o videos:** Imágenes y videos que contienen información estadística y geográfica;

IV. **Documentos de ofimática y metodologías:** Notas técnicas o análisis relacionados con la producción, administración y regulación de la Información Estadística y Geográfica, e

V. **Instrumentos de captación impresos:** Formatos en medio impreso que contienen los datos captados de los Informantes del Sistema para un Programa de Información.

Artículo 7.- La Escala de Calificación de Activos de información será de aplicación general y obligatoria para los Responsables de los Activos de información, con la finalidad de calificarlos con base en lo siguiente:

I. **Confidencialidad:**

a) Se considera nivel **alto** en Confidencialidad cuando el Activo de información cumpla al menos uno de los supuestos siguientes:

i. Contiene datos con identificadores correspondientes a las personas físicas o morales objeto de la Información, y

ii. Contiene datos o información que por Ley ha sido definida como confidencial, reservada o de divulgación restringida.

b) Se considera nivel **medio** en Confidencialidad cuando el Activo de información cumpla al menos uno de los supuestos siguientes:

i. Contiene datos individuales sin identificadores y su uso es interno;

ii. Contiene Conjuntos de Datos Captados o Procesados, o Productos de Información Estadística y Geográfica que aún no se han puesto a disposición del público, y

iii. Contiene información de uso interno que únicamente puede ser conocida por personal adscrito dentro de la misma Dirección de Área.

c) Se considera nivel **mínimo** en Confidencialidad cuando el Activo de información cumpla al menos uno de los siguientes supuestos:

i. Contiene Productos de Información Estadística y Geográfica de acceso público;

ii. Contiene información que por alguna Ley o acuerdo de la Junta de Gobierno ha sido determinada como de acceso público, y

iii. Cuando el Activo de información no cumpla con alguno de los supuestos establecidos en el nivel medio y alto.

II. Integridad:

a) Se considera nivel **alto** en Integridad cuando el Activo de información cumpla al menos uno de los siguientes supuestos:

i. Versiones finales de Productos y Presentaciones de Información Estadística y Geográfica, y

ii. Contiene Información de Interés Nacional o de otro tipo de Información que por Ley el Instituto debe conservar.

b) Se considera nivel **medio** en Integridad cuando el Activo de información cumpla al menos uno de los siguientes supuestos:

i. Contiene Conjuntos de Datos Captados o Procesados, Conjuntos de Información de contenido estadístico o geográfico, o Infraestructura de Información, y

ii. Contiene información relacionada al desarrollo de las actividades de las Unidades Administrativas transversales.

c) Se considera nivel **mínimo** en Integridad para los Activos de información que no cumplan alguno de los supuestos establecidos en el nivel medio y alto.

III. Disponibilidad:

a) Se considera nivel **alto** en Disponibilidad cuando el Activo de información cumpla al menos uno de los siguientes supuestos:

i. Contiene Productos de Información Estadística o Geográfica de acceso público cuya fecha y hora de publicación está definida en el Calendario de difusión de información estadística y geográfica y de Interés Nacional del INEGI, y

ii. Contiene aplicaciones informáticas o Repositorios comprometidos para las relaciones de promoción y colaboración del Instituto con otros sectores nacionales e internacionales.

b) Se considera nivel **medio** en Disponibilidad cuando el Activo de información cumpla al menos uno de los siguientes supuestos:

i. Contiene Conjuntos de Datos, Conjuntos de Datos Captados, Conjuntos de Datos Procesados, Conjuntos de Información o Infraestructura de Información, y

ii. Contiene aplicaciones informáticas o Repositorios internos de uso constante.

c) Se considera nivel **mínimo** en Disponibilidad para los Activos de información que no cumplan alguno de los supuestos establecidos en el nivel medio y alto.

Artículo 8.- Los Enlaces de Seguridad de la información deberán, en el ámbito de su competencia:

I. Coordinar la integración y actualización del Inventario de Activos de información;

II. Coordinar la integración del programa de implementación de los Controles correspondientes a los Activos de información críticos conforme a la calificación de éstos, y

III. Promover la identificación de los Activos de información correspondientes a los proyectos informáticos que se presenten ante el Grupo de Coordinación de TIC del Instituto Nacional de Estadística y Geografía.

Artículo 9.- Los Responsables de los Activos de información, en su ámbito de competencia deberán:

I. Mantener actualizado el Inventario de Activos de información con base en el Catálogo y la Escala de Calificación referidos en los artículos 6 y 7, respectivamente, y

II. Aprobar y coordinar la implementación de los Controles, que incrementen la Seguridad de los Activos de información bajo su responsabilidad conforme a la calificación de estos. Los casos en los que no se apliquen los Controles deberán justificarse y documentarse por medio de la aplicación informática determinada por la DGIAI para tal fin.

Sección II,
Inventario de Áreas de acceso restringido.

Artículo 10.- En la identificación de las Áreas de acceso restringido solamente se considerará a los inmuebles de uso permanente, excluyendo las instalaciones que el Instituto utiliza de manera temporal, como es el caso de los diferentes operativos censales o de levantamiento de encuestas. Se deberán considerar como Áreas de acceso restringido las que almacenan 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 CGI.

Artículo 11.- Las Unidades Administrativas productoras y transversales, las Direcciones Regionales y las Coordinaciones Estatales, a través de los Enlaces de Seguridad de la información, coordinarán de manera anual:

I. La integración y actualización del Inventario de Áreas de acceso restringido por medio de la aplicación informática determinada por la DGIAI para tal fin, y

II. La integración del programa de implementación de los Controles correspondientes a las Áreas de acceso restringido.

Artículo 12.- Los Responsables de las Áreas de acceso restringido, en su ámbito de competencia, deberán:

I. Mantener actualizado el Inventario de Áreas de acceso restringido, y

II. Aprobar y coordinar la implementación de Controles de seguridad de la información que incrementen la Seguridad en las Áreas de acceso restringido. Los casos en los que no se apliquen los Controles deberán justificarse y documentarse por medio de la aplicación informática determinada por la DGIAI para tal fin.

Artículo 13.- El Comité integrará y dará a conocer a la Dirección General Adjunta de Recursos Materiales y Servicios Generales el Inventario Institucional de Áreas de acceso restringido a partir de los inventarios que cada Unidad Administrativa y Dirección Regional apruebe.

Sección III,
Inventario de Requerimientos de Redundancia tecnológica.

Artículo 14.- Las Unidades Administrativas productoras, a través del Enlace de Seguridad de la información en coordinación con el Enlace Informático, deberán integrar y actualizar en el primer trimestre de cada año en el ámbito de su competencia, el Inventario de Requerimientos de Redundancia tecnológica relacionados con los Programas de Información por medio de la aplicación informática determinada por la DGIAI para tal fin.

Artículo 15.- El Enlace de Seguridad de la información, en colaboración con el Enlace Informático, coordinará la identificación de requerimientos de redundancia en los servicios tecnológicos con base en lo siguiente:

I. Los Programas de Información a realizarse en el año calendario posterior a la integración de éste, con el fin de que el área responsable de brindar el servicio de redundancia presupueste los recursos que resulten necesarios para ello;

II. Los Activos de información calificados con nivel alto en Disponibilidad;

III. Que sean considerados Procesos Críticos que generan Productos Esenciales, y

IV. Que el requerimiento no esté integrado en un esquema de redundancia ya implementado por la CGI.

Artículo 16.- El Inventario de Requerimientos de Redundancia tecnológica de cada Unidad Administrativa productora deberá contener al menos lo siguiente:

I. El Programa de Información y la o las Fases del proceso en las que se identifica la necesidad;

II. Los Activos de información calificados con nivel alto en Disponibilidad que estarán dentro de la cobertura de la redundancia;
III. El servicio tecnológico para el que se requiere redundancia, y
IV. El rango de fechas en el que se requiere la redundancia.

Artículo 17.- El Comité integrará y dará a conocer a la CGI el Inventario Institucional de Requerimientos de Redundancia tecnológica a partir de los inventarios que las Unidades Administrativas productoras aprueben en su ámbito de competencia.

Artículo 18.- El Enlace Informático se coordinará con el Enlace de Seguridad de la información correspondiente para:

I. Incluir los detalles técnicos de los requerimientos de redundancia tecnológica en el Programa Operativo Informático Anual, e
II. Identificar las necesidades de redundancia tecnológica en los proyectos informáticos que se presenten ante la CGI.

Sección IV,
Lista de Controles mínimos para la Seguridad de la información.

Artículo 19.- El Comité emitirá la Lista de Controles mínimos que se deben aplicar en los Activos de información críticos, la cual deberá ser revisada una vez al año con la finalidad de determinar su actualización. La Lista de Controles deberá contener:

I. Nombre, descripción, alcance y aplicación según el atributo de Seguridad al cual contribuyen a preservar, y
II. Evidencia que soporta su cumplimiento.

CAPÍTULO III,
Gestión de Incidentes de seguridad de la información

Sección I,
Notificación.

Artículo 20.- Todas las personas servidores públicos de las Unidades Administrativas productoras y transversales están obligados a reportar en términos de los presentes Lineamientos, cualquiera de los Eventos siguientes en torno a los Activos de información:

I. Pérdida total o parcial;
II. Alteración;
III. Acceso no autorizado;
IV. Divulgación no autorizada;
V. Falta de acceso;
VI. Cuando las condiciones del entorno supongan un factor de Riesgo para que se materialice alguno de los incisos anteriores;
VII. Cuando se presente alguna afectación a los Activos de información durante la modalidad de trabajo en oficina y Teletrabajo, y
VIII. Cualquier otra circunstancia que a juicio de las personas servidores públicos comprometa la Seguridad de los Activos de información.

Artículo 21.- La notificación de los Eventos descritos en el artículo anterior deberá realizarse a la brevedad a través de las alternativas siguientes:

I. Llamada telefónica a la Mesa de Ayuda Institucional;
II. Registro del reporte en la sección de Mesa de Ayuda en la Intranet del Instituto;
III. Envío de correo electrónico a la cuenta: mesa.ayuda@inegi.org.mx, y
IV. En caso de que las alternativas anteriores no estén disponibles, de manera personal al Enlace de Seguridad de la información de la Unidad Administrativa de su adscripción.

Artículo 22.- El reporte telefónico de los Eventos referidos en el artículo 20 de los presentes Lineamientos, se realizará a través del esquema de Mesa de Ayuda, a la extensión 5000 en la ciudad de Aguascalientes, al número telefónico 800 463 4402 a nivel nacional, así como en cada una de las extensiones de Mesa de Ayuda locales de cada Dirección Regional del Instituto, según sea la ubicación geográfica de la materialización del riesgo.

Artículo 23.- La DGIAI gestionará lo conducente para que el área responsable del Servicio de Mesa de Ayuda realice el registro de las notificaciones de Eventos de seguridad de la información.

Se deben registrar al menos los datos siguientes:

I. Fecha y hora en la que se recibe la notificación;

II. Modalidad: dentro de las oficinas del Instituto o Teletrabajo;

III. Entidad Federativa, Municipio o Demarcación Territorial. Para cuando sea en instalaciones del INEGI: edificio y oficina;

IV. Descripción del Evento;

V. Unidad Administrativa a la que pertenece el Activo de información relacionado con el Evento;

VI. Programa de Información afectado, en caso de que aplique;

VII. Activos de información involucrados;

VIII. Tipo de Evento:

a) Pérdida total o parcial;
b) Alteración;
c) Acceso no autorizado;
d) Divulgación no autorizada;
e) Falta de acceso;
f) Cuando las condiciones del entorno supongan un factor de Riesgo para que se materialice alguno de los incisos anteriores, y
g) Cualquier otra circunstancia que a juicio de las personas servidores públicos comprometa la Seguridad de la información.

Durante el registro de los Eventos se buscará tener la mayor cantidad de datos al respecto y son estrictamente necesarios para su atención inicial los datos a que se refieren las fracciones I al IV del presente artículo.

Artículo 24.- Los Enlaces de Seguridad de la información deberán registrar en la plataforma de Mesa de Ayuda las notificaciones de Eventos de Seguridad de la información que reciban de manera personal.

Artículo 25.- Las personas servidores públicos a cargo de la Mesa de Ayuda registrarán los reportes de Eventos de seguridad de la información en la plataforma correspondiente y, canalizarán su atención al Grupo de Respuesta a Incidentes de seguridad de la información.

Sección II,
Evaluación y toma de decisiones en torno a Eventos de seguridad de la información.

Artículo 26.- El Grupo de Respuesta a Incidentes de seguridad de la información estará conformado al menos por:

I. Las personas servidores públicos, con nivel jerárquico de subdirección y jefatura de departamento, adscritas a la Dirección de Seguridad y Confidencialidad de la Información;

II. Al menos un representante de la Dirección de Seguridad Informática;

III. Al menos un representante de la DGAANAR, y

IV. El Enlace de Seguridad de la información adscrito a la Unidad Administrativa en la que presente el Incidente.

Artículo 27.- El Grupo de Respuesta a Incidentes de seguridad de la información iniciará la atención de los Eventos de Seguridad de la información mediante las acciones siguientes:

I. Verificar que la situación reportada efectivamente se esté presentando;

II. Recabar las evidencias que soporten las acciones de verificación de la información, y

III. Conforme al impacto en la Confidencialidad, Integridad y Disponibilidad de los Activos de información, determinar si el Evento requiere ser considerado como un Incidente de seguridad de la información.

Artículo 28.- El Grupo de Respuesta a Incidentes de seguridad de la información cerrará el reporte de los Eventos que no sean considerados como Incidentes y en su caso informará al Área competente que deba dar seguimiento.

Artículo 29.- El Grupo de Respuesta a Incidentes de seguridad de la información, en coordinación con el Responsable del Activo de información afectado, determinarán el nivel de impacto del Incidente conforme a la escala siguiente:

I. Se considerará como nivel de impacto **alto** cuando el Incidente se caracterice por alguna de las situaciones siguientes:

a) Acceso o divulgación no autorizada de Activos de información calificados con un nivel alto en Confidencialidad;

b) Pérdida total o parcial, o alteración de los Activos de información calificados con un nivel alto en Integridad, y

c) Falta de acceso en Activos de información calificados con nivel alto en Disponibilidad.

II. Se considerará como nivel de impacto **medio** cuando el Incidente se caracterice por alguna de las situaciones siguientes:

a) Acceso o divulgación no autorizada de Activos de información calificados con un nivel medio en Confidencialidad;

b) Pérdida total o parcial, o alteración de Activos de información calificados con un nivel medio en Integridad;

c) Falta de acceso en Activos de información calificados con nivel medio en Disponibilidad.

III. Se considerará como nivel de impacto **mínimo** cuando el Incidente se caracterice por alguna de las situaciones siguientes:

a) Acceso o divulgación no autorizada de Activos de información calificados con un nivel mínimo en Confidencialidad;

b) Pérdida total o parcial, o alteración de Activos de información calificados con un nivel mínimo en Integridad, y

c) Falta de acceso en Activos de Información calificados con nivel mínimo en Disponibilidad.

Artículo 30.- El Grupo de Respuesta a Incidentes de seguridad de la información en la atención de los Incidentes calificados con un nivel de impacto alto, además de las acciones que se consideren pertinentes según las características del incidente, realizarán las acciones siguientes:

I. Informar la situación al Secretario Ejecutivo del Comité;

II. Solicitar la participación de las personas servidores públicos que resulten necesarios para la atención del Incidente;

III. De ser necesario, solicitar el apoyo de instancias externas, y

IV. Sugerir a la Unidad Administrativa productora o transversal a la que corresponda el Activo de Información afectado, a través de su Enlace de Seguridad de la información, la gestión de un comunicado a la sociedad o a las instancias que puedan resultar afectadas.

Sección III,
Respuesta a Incidentes de seguridad de la información.

Artículo 31.- El Grupo de Respuesta a Incidentes de seguridad de la información coordinará, con el Responsable del Activo de información correspondiente y las personas servidores públicos del Instituto que resulten pertinentes, las acciones para la atención del Incidente con base en lo siguiente:

I. Analizar las causas del Incidente;

II. Identificar los impactos en los diferentes ámbitos (personas, Información, económicos, operación, prestigio institucional, entre otros);

III. Identificar, reunir y resguardar las evidencias del Incidente;

IV. Reportar a las instancias correspondientes en cumplimiento a la normatividad aplicable;

V. Implementar las acciones que correspondan conforme a la documentación existente para casos de contingencia, recuperación de desastres, matrices de administración de riesgos u otro tipo de documentos similares en los que se determinen las acciones por realizar ante el Incidente en cuestión;

VI. En el caso de que no exista la documentación a la que se hace referencia en la fracción anterior, en el ámbito de las Unidades Administrativas productoras colaborar con el Actor Responsable de la Fase, en el ámbito de las Unidades Administrativas transversales colaborar con la persona servidor público con puesto de Dirección de Área que corresponda para determinar en el menor tiempo posible las líneas de acción para:

a) Detener la progresión del daño causado por el Incidente, y

b) Minimizar el impacto causado a las personas, la Información, la operación y el prestigio institucional. Se deberá considerar la participación de personas servidores públicos expertas en la temática dentro de la que se dio el Incidente, así como de prestadores de servicios.

Artículo 32.- Una vez que la respuesta al Incidente ha sido implementada, el Grupo de Respuesta a Incidentes de seguridad de la información realizará las acciones siguientes:

I. Informar al Secretario Ejecutivo del Comité, así como a las áreas afectadas o relacionadas con el Incidente;

II. Complementar los datos siguientes de la ficha de registro en la Mesa de Ayuda institucional:

a) Diagnóstico, es decir causas, vulnerabilidades y amenazas que ocasionaron el Incidente;
b) Impactos, en las personas, la Información, la operación, económico, prestigio institucional;
c) Respuesta al Incidente, es decir, conjunto de acciones implementadas para contrarrestar los daños;
d) Personal involucrado en la respuesta;
e) Posibles efectos colaterales;
f) Evidencias, y
g) Fecha de cierre de la atención del incidente.

Sección IV,
Aprendizaje de los Incidentes de seguridad de la información.

Artículo 33.- El Grupo de Respuesta de Incidentes de seguridad de la información deberá entregar al Secretario Ejecutivo del Comité, en un plazo no mayor a treinta días naturales contados a partir de la fecha de cierre de la atención del Incidente registrada en la Mesa de Ayuda institucional, el informe del resultado del análisis del mismo, lo anterior en coordinación con el Responsable del Activo de información correspondiente. El informe deberá contener al menos lo siguiente:

I. Probabilidad estimada de que el Incidente vuelva a ocurrir;
II. Vulnerabilidades y amenazas relacionadas con el Incidente, y
III. Propuesta de acciones para reducir la probabilidad de que el Incidente vuelva a ocurrir.

Artículo 34.- El Grupo de Respuesta a Incidentes de seguridad de la información informará, en el mes de noviembre al Secretario Ejecutivo del Comité, el resultado del análisis de los Incidentes de nivel mínimo y medio ocurridos en el año, con el objetivo de identificar los casos recurrentes y en su caso proponer las acciones correspondientes para reducir la probabilidad de ocurrencia o el impacto.

CAPÍTULO IV,
Líneas de acción de aplicación en las Fases del Proceso de Producción de Información Estadística y Geográfica

Sección I,
Líneas de acción de aplicación transversal.

Artículo 35.- El Actor del Rol Responsable de la Fase, en su ámbito de competencia, implementará acciones para proteger los Activos de información almacenados en equipos de cómputo móvil y medios de almacenamiento extraíbles, con base en lo siguiente:

I. Asegurar que se cuenta con el Respaldo de la información en las instalaciones del Instituto;
II. Establecer las condiciones que deben ser observadas para evitar el daño físico durante el transporte, y
III. Aplicar los Controles de seguridad que correspondan, según la calificación de los Activos de información.

Artículo 36.- El Responsable del activo de información, en su ámbito de competencia, deberá autorizar la asignación, modificación o eliminación de permisos de acceso a los Repositorios de información y a los Sistemas Informáticos considerando lo siguiente:

I. El acceso sólo se proporcionará a las personas servidores públicos, Personal externo y Prestadores de servicios que por razón de su empleo, cargo o comisión requieran acceder a ellos para el desarrollo de las actividades institucionales;
II. El nivel de acceso debe corresponder con las funciones y responsabilidades;
III. La integración de una lista donde se registren los permisos asignados;
IV. Dar a conocer por escrito a las personas servidores públicos, Personal externo y Prestadores de servicios a los que se les proporcione el acceso, la normatividad en la materia, así como de las consecuencias de incurrir en alguna de ellas, y
V. Revisar periódicamente la vigencia de los permisos de acceso.

Artículo 37.- El Actor del Rol Responsable de la Fase en su ámbito de competencia coordinará acciones a efecto de que se realicen respaldos de información con base en lo siguiente:

I. Identificar la información que requiere ser respaldada;
II. Definir el tipo de Respaldo que se necesite de acuerdo con lo siguiente:
a) Total: Copia la totalidad de los datos en otro medio de almacenamiento, y
b) Incremental: Copia de todos los archivos que han cambiado desde el último Respaldo;
III. Definir la frecuencia con la que se requiere que se realice el Respaldo;

IV. Definir los procedimientos por los que se accederán y utilizarán los respaldos;
V. Definir los períodos de retención de los respaldos, y
VI. Realizar pruebas de restauración de la información.

Artículo 38.- Las personas servidores públicos adscritas a las Unidades Administrativas productoras en la modalidad de Teletrabajo deberán:

I. Realizar el traslado de la información, los medios que la contienen y los Activos de Información de manera que se evite el robo, extravío o daño físico;
II. Mantener el espacio, donde se ubique la información, los medios que la contienen y los Activos de información, libre de sustancias y objetos que puedan ocasionar un daño a los mismos;
III. Utilizar únicamente las herramientas definidas institucionalmente para realizar reuniones virtuales, a menos que se trate de ámbitos de colaboración con otras instancias, y
IV. Cerrar la sesión y apagar la computadora cuando se deje de usar y guardar los soportes que contienen los Activos de información.

Sección II,
Seguridad de la información en la Fase de Documentación de Necesidades.

Artículo 39.- El Actor del Rol Responsable de la Fase de Documentación de Necesidades deberá:

I. Coordinar la identificación de los aspectos relacionados con la Seguridad de la información en lo que corresponde a las actividades específicas para la detección, gestión y aprobación de necesidades de los Programas de Información, y
II. Identificar en la normatividad aplicable los requisitos de Seguridad de la información que se deben cumplir, los cuales deberán formar parte de las evidencias de la fase y se deberán tomar en cuenta para el diseño de los Controles de seguridad de la información que se han de implementar durante todo el proceso de producción.

Sección III,
Seguridad de la información en la Fase de Diseño.

Artículo 40.- El Actor del Rol Responsable de la Fase deberá considerar la perspectiva de Seguridad de la información en las actividades siguientes:

I. Diseño de plataformas informáticas, componentes, aplicaciones y servicios de software necesarios para la producción de la información:

a) Elaborar la Matriz de Riesgos relacionados con las plataformas informáticas, componentes, aplicaciones y servicios de software donde se considere al menos los riesgos de acceso no autorizado, alteración, pérdida o falta de Disponibilidad de la Información;
b) Incluir la incorporación de características para mitigar los riesgos identificados en el numeral anterior, así como en los diferentes escenarios funcionales incluyendo el Teletrabajo, en su caso;
c) Especificar que las características a las que se refiere en el inciso anterior operen por defecto, es decir que su funcionamiento no dependa del usuario, y
d) Priorizar que la Información se resguarde en el Centro de Cómputo del Instituto.

II. Diseño de la captación:

a) Incluir en el Diseño de la captura de datos el uso de catálogos con claves que permitan anonimizar la captación de datos que representen un riesgo para preservar la confidencialidad estadística de los datos proporcionados por los Informantes del Sistema de manera que su respuesta se realice de forma anónima;
b) Incluir en los manuales operativos los aspectos necesarios para preservar la Seguridad de la información, considerando al menos:

   i. Las condiciones de uso de los instrumentos de captación impresos o electrónicos para proteger la información contenida en estos;
   ii. Las responsabilidades de cada figura operativa en cuanto a la Seguridad de la información a la que tienen acceso por motivo de sus funciones;
   iii. Las previsiones necesarias para preservar la Confidencialidad, Integridad y Disponibilidad, así como las sanciones en caso de incumplimiento;
   iv. Los procedimientos para aplicar Controles específicos para proteger la Confidencialidad, Integridad y Disponibilidad de la Información, y
   v. El procedimiento establecido para reportar los Eventos de la seguridad de la información.

III. Diseño del procesamiento y análisis de la producción. Incluir en el diseño de las estructuras y los sistemas para la creación de la base de datos y demás objetos de datos que constituyan el Conjunto de Información:

a) El periodo, la frecuencia y los tipos de respaldos;
b) La Información susceptible de transmitirse o almacenarse en forma cifrada;
c) Los sistemas y objetos de datos para los que se requiere la habilitación de bitácoras y el periodo de conservación de las mismas;

d) El periodo y los servicios tecnológicos en los que se requiere redundancia tecnológica;
e) El acceso mediante cuentas de usuario individuales, así como el mecanismo para que cada usuario cambie su contraseña en el primer inicio de sesión;
f) La lista de las personas servidores públicos que tendrán acceso, así como los permisos asignados, y
g) El procedimiento para la asignación, modificación o eliminación de permisos de acceso.

Artículo 41.- El Actor del Rol Responsable de la Fase en coordinación con el Enlace de Seguridad de la información presentará al Comité cuando así se solicite, un informe con los requerimientos y Controles de seguridad de la información que se definieron para todo el proceso.

Sección IV,
Seguridad de la información en la Fase de Construcción.

Artículo 42.- El Actor del Rol Responsable de la Fase deberá coordinar la integración de una lista que contenga los requerimientos en materia de Seguridad de la información, Controles y características identificadas en la Fase de Diseño, además de bitácoras de acceso a las bases de datos y a las herramientas informáticas diseñadas para la atención del proceso/proyecto.

La lista señalada en el párrafo anterior deberá formar parte de la documentación técnica del software conforme a lo establecido en el artículo 19 de la Norma Técnica.

Artículo 43.- El Actor del Rol Responsable de la Fase deberá comprobar que al finalizar la construcción o mejora de la infraestructura informática, componentes, aplicaciones y servicios de software necesarios para las Fases de Captación, Procesamiento, Análisis y Difusión se considere la inclusión de los elementos identificados y atendidos en la lista del artículo anterior.

Artículo 44.- El Actor del Rol Responsable de la Fase deberá identificar los Incidentes que se hayan presentado durante la prueba de campo o piloto para posteriormente integrarlos como parte del contenido del documento que contenga el análisis de la prueba piloto.

Artículo 45.- El Actor del Rol Responsable de la Fase deberá 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.

Sección V,
Seguridad de la información en la Fase de Captación.

Artículo 46.- El Actor del Rol Responsable de la Fase deberá coordinar las actividades siguientes:

I. Comprobar que los permisos de acceso a la información corresponden al personal que participa en la Fase de acuerdo con sus actividades;

II. Comprobar que los respaldos se realizan en tiempo y forma, así como el proceso de restauración de la información;

III. Comprobar que las bitácoras que se solicitaron se generan, conservan y pueden ser consultadas en el momento que sea necesario, e

IV. Incluir en el Esquema de captación, referido en el artículo 22 fracción II, inciso b), de la Norma Técnica, los temas de Seguridad de la información en los que se aborde al menos lo siguiente:

a) Las condiciones de uso para proteger la información contenida en los instrumentos de captación impresos o electrónicos;

b) Las responsabilidades de cada figura operativa en cuando a la Seguridad de la información a la que tienen acceso por motivo de sus funciones;

c) El carácter confidencial de los datos proporcionados por los Informantes, las previsiones necesarias para preservar dicha condición, así como las sanciones en caso de incumplimiento, ello conforme lo establecido en la Ley del Sistema Nacional de Información Estadística y Geográfica;

d) Los procedimientos para aplicar Controles específicos para proteger la Confidencialidad, Integridad y Disponibilidad de la Información, y

e) El procedimiento establecido para reportar los Eventos de la Seguridad de la información.

Sección VI,
Seguridad de la información en la Fase de Procesamiento.

Artículo 47.- El Actor del Rol Responsable de la Fase deberá implementar acciones para que la imagen de los datos integrados, referida en el artículo 26 fracción I de la Norma Técnica, sea tal cual como fueron recibidos en la Fase de Captación:

I. Se almacene en forma cifrada, y

II. Se defina y verifique el funcionamiento del procedimiento de recuperación.

Artículo 48.- El Actor del Rol Responsable de la Fase deberá coordinar que durante el desarrollo de las actividades que corresponden al procesamiento, se revisen las bitácoras de los accesos a las bases de datos y aplicaciones informáticas para identificar posibles Eventos de Seguridad de la información.

Artículo 49.- Cuando a raíz de la revisión de las bitácoras a las que se refiere en el artículo anterior, se identifiquen datos a partir de los cuales se pueda advertir una afectación a la

Confidencialidad, Integridad y Disponibilidad de la información, el Actor del Rol Responsable de la Fase deberá hacerlo del conocimiento del Actor del Rol Responsable de Proceso y del Enlace de Seguridad de la información quien a su vez valorará si el hecho deba ser reportado como un Evento de seguridad de la información.

Sección VII,
Seguridad de la información en la Fase de Análisis de Producción.

Artículo 50.- Para reducir la posibilidad de una fuga de información o publicación anticipada, el Actor del Rol Responsable de la Fase deberá determinar a las personas servidores públicos que tengan acceso a los Conjuntos de Información, Conjuntos de Datos con controles de difusión, Conjuntos de Datos agregados, Indicadores Objetivo, otros indicadores, Metadatos y contenido adicional relevante.

Sección VIII,
Seguridad de la información en la Fase de Difusión.

Artículo 51.- El Actor del Rol Responsable de la Fase deberá coordinar las acciones para verificar que previo a la fecha y hora establecidos para la publicación de la información se cuenta con acceso a los sistemas o portales definidos por la Dirección General de Comunicación, Servicio Público de Información y Relaciones Institucionales para realizar la publicación de la Información.

Artículo 52.- El Actor del Rol Responsable de la Fase deberá coordinar las acciones para verificar que posterior a la hora establecida para la publicación de la información los datos, metadatos y metodologías publicados están legibles, completos y corresponden a la versión liberada en la fase anterior.

Artículo 53.- El Actor del Rol Responsable de la Fase deberá incorporar el resultado y los detalles de las actividades correspondientes a esta sección en el reporte señalado en el artículo 33 fracción II de la Norma Técnica.

Sección IX,
Seguridad de la información en la Fase de Evaluación del Proceso.

Artículo 54.- El Actor del Rol Responsable de la Fase deberá incorporar en el reporte de evaluación referido en el artículo 35 de la Norma Técnica lo siguiente:

I. Lista de Controles de seguridad de la información aplicados en cada Fase del proceso;

II. Situaciones internas o externas que hayan puesto en riesgo la Confidencialidad de los datos proporcionados por los Informantes del Sistema;

III. Incidentes de seguridad de la información que hayan ocurrido en el desarrollo del ciclo del Programa de Información, y

IV. Propuesta de adecuaciones para contrarrestar las situaciones a las que se refieren las dos fracciones anteriores.

Sección X,
Del resguardo de evidencias.

Artículo 55.- Las evidencias de la implementación de lo establecido en el presente capítulo, deberán almacenarse con el resto de las evidencias de la aplicación de la Norma Técnica.

CAPÍTULO V,
Líneas de acción de aplicación para las Unidades Administrativas transversales.

Artículo 56.- Corresponde a las personas servidores públicos con puesto de Dirección de Área, en su ámbito de competencia, en el diseño de las plataformas informáticas, los componentes, las aplicaciones y los servicios de software, coordinar las acciones siguientes:

I. Elaborar la Matriz de Riesgos relacionados con las plataformas informáticas, componentes, aplicaciones y servicios de software donde se considere al menos los riesgos de acceso no autorizado, alteración, pérdida o falta de Disponibilidad de la Información;

II. Incluir la incorporación de características para administrar los riesgos identificados en el numeral anterior, así como en los diferentes escenarios funcionales incluyendo el Teletrabajo, en su caso;

III. Especificar que las características a las que se refiere en la fracción anterior operen por defecto, es decir que su funcionamiento no dependa del usuario;

IV. Priorizar que la Información se resguarde en el Centro de Cómputo del Instituto;

V. Definir la Información susceptible de transmitirse o almacenarse en forma cifrada;

VI. Establecer el periodo y los servicios tecnológicos en los que se requiere redundancia tecnológica;

VII. Habilitar el acceso mediante cuentas de usuario individuales, así como el mecanismo para que cada usuario cambie su contraseña en el primer inicio de sesión;

VIII. Elaborar la lista de las personas servidores públicos que tendrán acceso, así como los permisos asignados, y

IX. Definir y socializar el procedimiento para la asignación, modificación, o eliminación de permisos de acceso.

Artículo 57.- Corresponde a las personas servidores públicos con puesto de Dirección de Área, en su ámbito de competencia, coordinar las acciones para proteger los Activos de información almacenados en equipos de cómputo móvil y medios de almacenamiento extraíbles, con base en lo siguiente:

I. Asegurar que se cuenta con el Respaldo de la información en las instalaciones del Instituto;
II. Establecer las condiciones que deben ser observadas para evitar el daño físico durante el transporte, y
III. Aplicar los Controles de seguridad que correspondan, según la calificación de los Activos de información.

Artículo 58.- El Responsable del activo de información, en su ámbito de competencia, deberá autorizar la asignación, modificación o eliminación de permisos de acceso a los Repositorios de información y a los Sistemas Informáticos considerando lo siguiente:

I. El acceso sólo se proporcionará a las personas servidores públicos, Personal externo y Prestadores de servicios que por razón de su empleo, cargo o comisión requieran acceder a ellos para el desarrollo de las actividades institucionales;
II. El nivel de acceso debe corresponder con las funciones y responsabilidades;
III. La integración de una lista donde se registren los permisos asignados;
IV. Dar a conocer a las personas servidores públicos, Personal externo y Prestadores de servicios a los que se les proporcione el acceso, la normatividad en la materia, así como de las consecuencias de incurrir en alguna de ellas, y
V. Revisar periódicamente la vigencia de los permisos de acceso.

Artículo 59.- Corresponde a las personas servidores públicos con puesto de Dirección de Área, en su ámbito de competencia, coordinar que se realicen respaldos de información con base en lo siguiente:

I. Identificar la información que requiere ser respaldada;
II. Definir el tipo de Respaldo que se necesite de acuerdo con lo siguiente:
   a) Total: Copia la totalidad de los datos en otro medio de almacenamiento, y
   b) Incremental: Copia de todos los archivos que han cambiado desde el último Respaldo;
III. Definir la frecuencia con la que se requiere que se realice el Respaldo;
IV. Definir los procedimientos por los que se accederán y utilizarán los respaldos;
V. Definir los períodos de retención de los respaldos, y

VI. Realizar pruebas de restauración de la información.

Artículo 60.- Las personas servidores públicos adscritas a las Unidades Administrativas transversales, en la modalidad de Teletrabajo deberán:

I. Realizar el traslado de la información, los medios que la contienen y los Activos de Información de manera que se evite el robo, extravío o daño físico;
II. Mantener el espacio, donde se ubique la información, los medios que la contienen y los Activos de información, libre de sustancias y objetos que puedan ocasionar un daño a los mismos;
III. Utilizar únicamente las herramientas definidas institucionalmente para realizar reuniones virtuales, a menos que se trate de ámbitos de colaboración con otras instancias, y
IV. Cerrar la sesión y apagar la computadora cuando se deje de usar y guardar los soportes que contienen los Activos de información.

Artículo 61.- Corresponde a las personas servidores públicos con puesto de Dirección de Área, en su ámbito de competencia, reunir y resguardar las evidencias de la implementación de lo establecido en el presente capítulo.

INTERPRETACIÓN

Artículo 62.- Corresponde al titular de la Dirección General de Integración, Análisis e Investigación la interpretación de los Lineamientos para efectos administrativos.

Corresponderá al Comité resolver los casos no previstos en los Lineamientos.

TRANSITORIOS

ÚNICO.- Los Lineamientos entrarán en vigor al día hábil siguiente de su publicación en la Normateca Institucional.

El presente documento fue aprobado en la Sesión Ordinaria 01 del Comité de Seguridad y Confidencialidad Estadística de la Información, celebrada el día 7 de abril de 2021, mediante Acuerdo CSCEI-003/ORD-1/2021.

Última hoja de los Lineamientos de Seguridad de la Información Estadística y Geográfica del Instituto Nacional de Estadística y Geografía, el cual se hace constar de 26 fojas útiles y fue publicado en la Normateca Institucional con fecha 19 de abril de 2021.