INSTITUTO NACIONAL
DE ESTADÍSTICA Y GEOGRAFÍA

LINEAMIENTOS PARA EL FORTALECIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN EN LOS PROCESOS Y SERVICIOS INSTITUCIONALES.

COMITÉ DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN.

JULIO 2015.
Aguascalientes, Aguascalientes.

ÍNDICE

INTRODUCCIÓN

El Instituto Nacional de Estadística y Geografía (Instituto) reconoce la importancia de proteger la información estadística y geográfica ya sea generada por el Instituto o entregada por terceros, así como aquella propia de la gestión institucional, con fundamento en el artículo 4 de la Ley del Sistema Nacional de Información Estadística y Geográfica, y la importancia de la conservación y el resguardo de la información en términos de lo dispuesto por los artículos 37, 38 y 47 del citado ordenamiento a efecto de preservar los principios de confidencialidad y reserva establecidos por los mismos.

En el Instituto se han realizado esfuerzos encaminados a fortalecer el cuidado de la Información, destacando las iniciativas en materia informática, así como el Sistema Integral de Archivos y las medidas de protección y acceso a los inmuebles.

El activo más valioso para el Instituto, después de los servidores públicos, es la información, el cuidado de la misma depende de todos los colaboradores del mismo y corresponde al Titular de cada Unidad Administrativa definir y asegurar los procedimientos específicos que fortalezcan la Seguridad de la Información relacionada con los procesos a su cargo.

El Sistema de Seguridad de la Información tiene por objeto promover y coordinar la Seguridad de la Información en los procesos institucionales, así mismo le corresponde al Comité del Sistema de Seguridad de la Información definir los lineamientos a través de los cuales se fortalecerá la confidencialidad, integridad y disponibilidad de la Información en un marco de mejora continua.

Por lo anterior, con fundamento en el numeral 4 del Apartado h.2 de las Políticas para la Seguridad de la Información del Instituto Nacional de Estadística y Geografía, el Comité del Sistema de Seguridad de la Información tiene a bien emitir los siguientes:

LINEAMIENTOS PARA EL FORTALECIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN EN LOS PROCESOS Y SERVICIOS INSTITUCIONALES.

CAPÍTULO I,
Lineamientos Generales.

Artículo 1. Los presentes Lineamientos tienen por objeto establecer las disposiciones a partir de las cuales las Unidades y Áreas Administrativas del Instituto, al amparo de su ámbito de competencia, instrumentarán las medidas técnicas y organizativas para fortalecer la Seguridad de la Información en los procesos, proyectos y servicios institucionales, contribuyendo a preservar la Confidencialidad, Integridad y Disponibilidad de la Información.

Artículo 2. Los presentes Lineamientos, son de observancia general y obligatoria para los servidores públicos adscritos en las Unidades y Áreas Administrativas del Instituto, corresponde a los Titulares implementarlas y promover su cumplimiento en su respectivo ámbito de competencia.

Artículo 3. El Comité del Sistema de Seguridad de la Información es el encargado de normar los aspectos generales y los particulares transversales en materia de Seguridad de la Información, mientras que los aspectos particulares serán normados por los titulares de las siguientes Unidades y Áreas Administrativas:

I. Dirección General Adjunta de Informática: Aspectos relacionados con las tecnologías de la información, en específico, aspectos de Seguridad Informática;
II. Dirección General Adjunta de Recursos Materiales y Servicios Generales: Aspectos relacionados con la seguridad física y el resguardo de documentos en papel;
III. Dirección General Adjunta de Programación, Organización y Presupuesto: Aspectos relacionados con la reserva de información, y
IV. Contraloría Interna: Aspectos de Control interno y gestión de riesgos.

Artículo 4. Se consideran aspectos transversales en materia de Seguridad de la Información todos aquellos que por su naturaleza no resulte de competencia directa de las Unidades y Áreas Administrativas mencionadas en el artículo anterior, cuya atención requiera de la colaboración de dos o más Unidades o Áreas Administrativas. Para efectos de lo dispuesto por los Lineamientos, se consideran aspectos transversales en forma enunciativa, más no limitativa, los siguientes:

I. Criterios generales para la protección y resguardo de la Información con base en sus contenidos;
II. Criterios para la calificación de activos de información;
III. Listado de activos de información generada por el INEGI, y

IV. Los demás que derivados de las necesidades institucionales sean considerados como tales por el Comité del Sistema de Seguridad de la Información.

Artículo 5. El Comité del Sistema de Seguridad de la Información podrá sugerir a las Unidades y Áreas Administrativas la emisión de disposiciones normativas en el ámbito de su competencia, que tengan por objeto regular aspectos que deban ser atendidos en materia de Seguridad de la Información.

Artículo 6. Resultan aplicables los conceptos contenidos en el numeral I, denominado: Glosario de las Políticas para la Seguridad de la Información del Instituto Nacional de Estadística y Geografía, así mismo para efectos de los presentes Lineamientos se entenderá por:

I. **Acceso Privilegiado:** Permisos otorgados a una cuenta de usuario para que acceda a información o funciones de administración, mantenimiento o configuración;

II. **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;

III. **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización;

IV. **Aplicación, o Aplicaciones Informáticas:** Sistemas informáticos o software, que se conforman por un conjunto de componentes o programas construidos con herramientas de software que habilitan una funcionalidad o automatizan un proceso, de acuerdo a requerimientos previamente definidos;

V. **Autenticación:** Proceso mediante el cual se establece el nivel de confianza recíproca suficiente sobre la identidad del usuario y el Instituto;

VI. **Comité:** El Comité del Sistema de Seguridad de la Información;

VII. **Enlace de Seguridad de la Información:** Servidor público del Instituto, designado por el Titular de cada unidad administrativa como su representante ante el Comité;

VIII. **Incidente de Seguridad de la Información:** Hecho que sucede de manera inesperada, materializando un riesgo que afecta a la Seguridad de la Información;

IX. **Instituto:** Instituto Nacional de Estadística y Geografía;

X. **Lineamientos:** Lineamientos para el Fortalecimiento de la Seguridad de la Información en los Procesos y Servicios Institucionales;

XI. **Medios de Almacenamiento:** Es el material físico donde se almacenan los datos electrónicos, tales como: discos compactos, DVD, Memorias USB, Discos duros externos;

XII. **Redundancia**: 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;

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

XIV. Seguridad de la Información: Capacidad de preservar la Confidencialidad, Integridad y Disponibilidad de la Información a partir de la implementación de medidas técnicas y organizativas, y

XV. Uso Inadecuado (de Información): Violación a disposiciones normativas y administrativas establecidas para el uso de la Información, y que por lo tanto pone en riesgo la propia Información, al proceso, al Instituto o a terceros.

Artículo 7.- Los Titulares de las Unidades Administrativas deben informar al Comité por escrito, sobre los servidores públicos del Instituto que por el ámbito de competencia de sus funciones estén facultados para mantener contacto con grupos de interés o foros en los que se traten temas o proyectos relacionados con Seguridad de la Información a efecto de:

I. Mejorar el conocimiento y mantener actualizado al Instituto sobre las mejores prácticas relacionadas con la Seguridad de la Información;

II. Recibir alertas tempranas respecto a amenazas globales o regionales en materia de Seguridad de la Información;

III. Acceder a foros, consejos y otros grupos de expertos en materia de Seguridad de la Información, y

IV. Establecer acuerdos de intercambio de información para mejorar la cooperación, la coordinación y la asesoría en materia de Seguridad de la Información.

Artículo 8.- Los servidores públicos del Instituto, exceptuando los que formen parte del Comité y del Grupo de Apoyo, facultados por los Titulares de las Unidades Administrativas con relación a lo expresado en el artículo 4, deben informar por escrito al Enlace de Seguridad de la Información, correspondiente a la Unidad Administrativa de su adscripción, las actividades que se realicen derivadas del contacto con los grupos de interés u otros foros de Seguridad de la Información.

Artículo 9.- Las Unidades y Áreas Administrativas, de acuerdo a lo establecido por las Normas de Control Interno para el Instituto Nacional de Estadística y Geografía, deberán hacer la identificación de los Riesgos de Seguridad de la Información que se pudieran presentar durante los procesos, proyectos o servicios de los que sean responsables.

CAPÍTULO II,
GESTIÓN DE ACTIVOS DE INFORMACIÓN.

Sección I,
Responsabilidad de los Activos de Información.

Artículo 10.- Las Unidades y Áreas Administrativas deben clasificar la información, independientemente del medio que la contenga, conforme a lo especificado en la legislación y normatividad administrativa vigentes en materia de archivos, considerando para ello lo dispuesto por los Lineamientos y demás criterios emitidos por el Comité.

Artículo 11.- Los responsables de procesos institucionales, al amparo de sus atribuciones, deben definir:

I. A los servidores públicos que tendrán bajo custodia la Información;
II. La Información a la que se brinda el acceso conforme a la normatividad que le resulte aplicable;
III. El acceso a la Información por parte de los servidores públicos del Instituto, Personal Externo y Prestadores de Servicios, independientemente del medio en que esté almacenada, y
IV. El tiempo por el que se brinda el acceso a la Información.

Artículo 12.- Cada servidor público del Instituto deberá realizar acciones tendientes a:

I. Verificar que la Información correspondiente a su ámbito de competencia es clasificada e inventariada conforme a la legislación y normatividad administrativa vigente en materia de archivos considerando en lo conducente lo dispuesto por los Lineamientos y demás criterios que emita el Comité;
II. Observar puntualmente la normatividad aplicable en materia de seguridad informática;
III. Cumplir con la normatividad en materia de seguridad física y el resguardo de documentos;
IV. Mantener la confidencialidad y resguardo de la Información bajo su resguardo;
V. Observar puntualmente la normatividad en materia de Control de Interno, conforme a la administración de riesgos;
VI. Verificar que el manejo de los Activos de Información en su destrucción se realiza conforme a la normatividad administrativa aplicable en la materia, y
VII. Atender cualquier otra recomendación del Comité en materia de Seguridad de la Información.

Artículo 13.- Las Unidades y Áreas Administrativas deberán establecer acciones para que los servidores públicos de su adscripción, Personal Externo y Prestadores de Servicios, conozcan los requisitos de seguridad para acceder o hacer uso de los Activos de Información.

Sección II,
Manejo de los Activos de Información.

Artículo 14.- Los servidores públicos responsables de la Información, en las acciones de manejo de los Medios de Almacenamiento, deben considerar:

I. La salida de los Activos de Información solamente se debe realizar en los casos en que sea necesario para el desarrollo de actividades institucionales, para lo cual será necesario cubrir los aspectos definidos en la normatividad administrativa aplicable;

II. Asegurar que se cuenta con al menos una copia de la Información que permanezca en las instalaciones del Instituto;

III. Aplicar las medidas de protección de acceso a la Información que correspondan de acuerdo a la naturaleza del Activo de Información conforme a la normatividad vigente, y

IV. Asegurar la destrucción de la Información cuando esta ya no sea de utilidad para el Instituto, conforme a la normatividad aplicable en la materia.

Artículo 15.- Las Unidades y Áreas Administrativas deben considerar para el transporte de los Activos de Información lo siguiente:

I. Medios que protejan los Activos de Información de cualquier daño físico durante su transporte, y

II. Verificar que se cumplen con las condiciones de seguridad para la Información cuando el transporte de los Activos de Información sea a través de Personal Externo.

Artículo 16.- Los servidores públicos del Instituto solamente deberán almacenar la Información de carácter institucional en los medios y servicios institucionales dispuestos para tal fin.

CAPÍTULO III,
CONTROL DE ACCESOS A ACTIVOS DE INFORMACIÓN.

Sección I,
Control de Accesos.

Artículo 17.- Los responsables de procesos institucionales deben considerar lo siguiente para permitir o denegar el acceso a los Activos de Información correspondientes a su ámbito de competencia:

I. El acceso a los Activos de Información sólo se proporcionará a los servidores públicos, Personal Externo y Prestadores de Servicios que por razón de su empleo, cargo o comisión tengan la necesidad de acceder a ellos para el desarrollo de las actividades Institucionales;

II. Deberá darse a conocer a los servidores públicos, Personal Externo y Prestadores de Servicios a los que se les proporcione el acceso a los Activos de Información las situaciones que son consideradas como Uso Inadecuado, así como de las consecuencias de incurrir en alguna de ellas, y

III. Deberán establecerse medidas de control de acceso físico y lógico para reducir la probabilidad de que los Activos de Información sean accedidos por personal no autorizado, dichos controles deberán cumplir con los requisitos de seguridad propios del tipo de Información, así como de los requerimientos legales y administrativos correspondientes.

Sección II,
Gestión de Acceso de los Usuarios.

Artículo 18.- Las Unidades y Áreas Administrativas en las acciones de control de la asignación, modificación y revocación de los permisos de acceso que se otorguen a los servidores públicos, Personal Externo y Prestadores de Servicios, sobre cualquier medio o mecanismo que proporcione acceso a los Activos de Información del Instituto:

I. La correspondencia entre el nivel de acceso, las funciones y responsabilidades de los distintos usuarios de Activos de Información;

II. Contar con un registro de los permisos de acceso concedidos a Activos de Información que se encuentren dentro del Listado de Activos de Información del INEGI;

III. Los cambios de adscripción, funciones, responsabilidades y la conclusión de la relación con el Instituto, y

IV. Revisión periódica de los permisos de acceso concedidos.

Artículo 19.- Las Unidades Administrativas establecerán acciones de control a los Activos de Información que conforme a los criterios que emita el Comité deban contar con permisos de Acceso Privilegiado, considerando:

I. Los derechos de Acceso Privilegiado deben asignarse únicamente a los servidores públicos, Personal Externo y Prestadores de Servicios que los requieran para desarrollar las actividades institucionales que les son encomendadas de acuerdo con su cargo o comisión;

II. Un análisis de la asignación, revisión, ratificación y retiro del Acceso Privilegiado;

III. Mantener un registro actualizado de las asignaciones de Acceso Privilegiado;

IV. Los permisos de Acceso Privilegiado deberán registrarse y controlarse por medios que permitan identificar el uso de los Activos de Información que requieran dicho trato, y

V. La vigencia de la asignación de permisos de Acceso Privilegiado deben revisarse periódicamente, según lo defina cada Unidad y Área Administrativa, con el objetivo de verificar que los permisos asignados corresponden a las necesidades y competencias de los servidores públicos a los que se les asignaron los permisos.

Artículo 20.- Las Unidades y Áreas Administrativas que por motivo de sus funciones administren cualquier tipo de mecanismo de autenticación deberán considerar las medidas necesarias para asegurar el resguardo de la Información correspondiente a los medios de acceso a los mismos haciendo del conocimiento de los usuarios de los mismos la responsabilidad que asumen sobre el uso de los mismos para el ejercicio de actividades a su cargo, con el objeto de favorecer su efectividad, en cumplimiento a las disposiciones que al efecto emita la Dirección General Adjunta de Informática.

Artículo 21.- Las Unidades y Áreas Administrativas deberán establecer medidas técnicas y organizativas a efecto de que los derechos de acceso de los servidores públicos del Instituto y Personal Externo y Prestadores de Servicios, a los Activos de Información, instalaciones de procesamiento de la Información y áreas de acceso restringido les sean retirados a la terminación de su empleo, contrato o convenio, o ajustarse al cambio de sus funciones.

Sección III,
Control de Acceso a Mecanismos de Acceso a los Activos de Información

Artículo 22.- Las Unidades y Áreas Administrativas en las acciones de control de acceso a cualquier mecanismo que proporcione acceso a Activos de Información deberán establecer medidas que faciliten el resguardo de los medios físicos y electrónicos de acceso y operación de los mismos en cumplimiento a las disposiciones que al efecto emita la Dirección General Adjunta de Informática.

CAPÍTULO IV,
PROTECCIÓN DE ACCESO A CONTENIDOS DE ACTIVOS DE INFORMACIÓN.

Artículo 23.- Los servidores públicos del Instituto deberán de aplicar los mecanismos definidos por la legislación y normatividad administrativa aplicable atendiendo a la naturaleza de la Información de cuyo resguardo sean responsables con el objeto de asegurar la protección, resguardo y acceso a los contenidos de Activos de Información en el desempeño de las atribuciones o funciones de su competencia.

Artículo 24.- Corresponde a las Unidades y Áreas Administrativas identificar en sus respectivos ámbitos de competencia, la Información que sea necesario proteger de manera especial conforme al Listado de activos de información del INEGI que emita el Comité en términos de los Lineamientos, aplicando los mecanismos que resulten necesarios en cumplimiento a la legislación y normatividad administrativa aplicable, conforme a la naturaleza del o los Activos de Información cuya administración o uso se encuentren a su cargo.

CAPÍTULO V,
SEGURIDAD FÍSICA Y AMBIENTAL.

Sección I,
Áreas de Acceso Restringido.

Artículo 25.- El Comité acordará y dará a conocer a la Dirección General Adjunta de Recursos Materiales y Servicios Generales el Listado de Áreas de Acceso Restringido del Instituto con la finalidad de que se establezcan las medidas pertinentes para controlar el acceso a éstas con el objeto de garantizar la Seguridad de la Información.

Artículo 26.- Las Unidades y Áreas Administrativas deberán definir los requisitos que quienes tengan acceso a Áreas de Acceso Restringido atendiendo a la naturaleza de la Información que se resguarde en las mismas en ejercicio de las atribuciones de su competencia.

CAPÍTULO VI,
SEGURIDAD EN LAS OPERACIONES.

Sección I,
Responsabilidades y Procedimientos de Operación.

Artículo 27.- Cuando las Unidades y Áreas Administrativas realicen cambios en su organización, distribución de cargos, de trabajo o adecuaciones a los procesos o instalaciones deberán tomar en consideración lo siguiente:

I. La evaluación de los impactos potenciales en la Seguridad de la Información;
II. La verificación de que se cumplen los requisitos de Seguridad de la Información;
III. Acciones de recuperación de los cambios fallidos e imprevistos, y
IV. Las demás que a juicio del Comité resulten necesarias para resguardar la Seguridad de la Información.

Sección II,
Respaldos de Activos de Información.

Artículo 28.- Corresponde a las Unidades y Áreas Administrativas implementar acciones a efecto de que se realicen copias de la Información relacionada con los procesos, proyectos y servicios de su competencia, debiendo tomar para ello en cuenta las siguientes consideraciones:

I. Identificar la Información que requiere ser respaldada y tipo de Respaldo que se necesite de acuerdo a 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;

II. Definir la frecuencia de los respaldos conforme a las necesidades de los procesos, los requisitos de Seguridad de la Información involucrada y la criticidad de la Información para la continuidad del funcionamiento del Instituto;
III. Integrar y mantener actualizada una bitácora en la que se registren los Respaldos realizados, ubicación, fecha, hora y descripción de la Información contenida;
IV. Definir los procedimientos por los que se accederán y utilizaran los respaldos;
V. Los Respaldos deben ser almacenados en una ubicación remota, a una distancia en la que los daños en el sitio principal no le afecten;
VI. Los Medios de Almacenamiento que contengan los Respaldos deben ser probados regularmente para asegurarse de que pueden ser usados cuando se requiera;
VII. Realizar pruebas de restauración de la Información;
VIII. La Información confidencial debe respaldarse cuidando que se incorporen los mecanismos de protección aplicables conforme a su naturaleza, y
IX. Tomar las previsiones necesarias para propiciar la debida observancia de la legislación y normatividad administrativa aplicables en materia de Seguridad de la Información.

Sección III,
Registros de eventos y Monitoreo.

Artículo 29.- Las Unidades y Áreas Administrativas responsables de mecanismos que proporcionen acceso a Activos de Información que se encuentren contenidos en el Listado de Activos de Información del INEGI deberán registrarlos ante el Comité, proporcionando para ello la siguiente información:

I. Nombre que identifique al mecanismo;
II. Tipo de mecanismo (procedimiento, aplicación informática, entre otros);
III. Objetivo;
IV. Descripción detallada de su funcionalidad, uso y alcances;
V. Descripción de los Activos de Información accedidos y operaciones que se facilitan (incorporación, borrado, modificación, entre otros);
VI. Descripción de los mecanismos de protección de Activos de Información incluidos;

VII. Mecanismos de activación o desactivación de los mecanismos de protección en caso de que se incluyan;
VIII. Medidas de monitoreo y atención a los mecanismos de protección;
IX. Esquemas de continuidad y recuperación ante contingencias;
X. Resultados del análisis de riesgos realizado, y
XI. Otros aspectos relevantes del mecanismo que a consideración del responsable deban ser aclarados con respecto al manejo de Activos de Información.

Artículo 30.- En el registro de eventos sobre uso de mecanismos que proporcionen acceso a Activos de Información que se encuentren contenidos en el Listado de Activos de Información del INEGI deberá mantenerse una bitácora, con los siguientes datos:

I. Identificar a los servidores públicos autorizados para su uso;
II. Las actividades realizadas;
III. Las fechas y horarios de los ingresos y salidas al mecanismo;
IV. Situaciones anómalas relacionadas con el acceso al mecanismo;
V. Cualquier cambio en la forma de operación del mecanismo;
VI. Registros de las transacciones realizadas por los usuarios, y
VII. Las demás que determine la Unidad o Área Administrativa a cargo de los mecanismos, atendiendo a la naturaleza de la Información contenida en el mismo en cumplimiento a la legislación y normatividad aplicables.

Artículo 31.- Los registros de eventos sobre uso de mecanismos que proporcionen acceso a Activos de Información señalados en el artículo anterior deberán protegerse contra:

I. Las modificaciones de los eventos que se registran;
II. Edición o destrucción de la Información que contienen;
III. Capacidad suficiente para mantener al menos tres meses de eventos registrados, y
IV. Las demás que determine la Unidad o Área Administrativa a cargo de los mecanismos, atendiendo a la naturaleza de la Información contenida en el mismo en cumplimiento a la legislación y normatividad aplicables.

Sección IV,
Control de Mecanismos de Acceso a Activos de Información en Operación.

Artículo 32.- Los servidores públicos responsables de los mecanismos de acceso a los Activos de Información vigilarán se mantenga su correcta operación y en caso necesario aplicar las medidas correctivas correspondientes, atendiendo a lo dispuesto por los Lineamientos, la legislación y normatividad administrativa aplicables, conforme a la naturaleza del mecanismo de que se trate.

Sección V,
Gestión de Vulnerabilidades Técnicas.

Artículo 33.- En la identificación de vulnerabilidades técnicas de los mecanismos que accedan a Activos de Información contenidos en el Listado de Activos de Información del INEGI, las Unidades y Áreas Administrativas y servidores públicos responsables de los mismos, deberán considerar:

I. Una vez que una vulnerabilidad técnica haya sido ubicada, deberán identificar los riesgos asociados y las medidas que deben adoptarse;

II. Los Riesgos asociados con las medidas correctivas a aplicar;

III. Las pruebas previas a las medidas correctivas a aplicar para evitar daños en los Activos de Información;

IV. En caso de requerirse:

a) Desactivar servicios relacionados con la vulnerabilidad;
b) La adaptación o la adición de controles de acceso, y
c) El aumento de la vigilancia para detectar ataques reales basados en la vulnerabilidad detectada;

V. Integrar y mantener actualizada una bitácora en la que se registren las vulnerabilidades;

VI. Verificar y evaluar de manera periódica las acciones implementadas para corregir las vulnerabilidades con el fin de comprobar la efectividad de éstas, y

VII. Las demás que determine la Unidad o Área Administrativa a cargo del mecanismo, en el que haya sido detectada la vulnerabilidad, atendiendo a la naturaleza de la Información contenida en el mismo en cumplimiento a la legislación y normatividad aplicables.

Sección VI,
Transferencia de Información.

Artículo 34.- En las acciones concernientes a la transferencia de Información, a través de cualquier medio, se deberá atender las normas Institucionales que apliquen conforme a la naturaleza de los medios utilizados con el objeto de garantizar y mantener la Seguridad de la Información.

Sección VII,
Uso de Datos de prueba.

Artículo 35.- En las acciones relacionadas con la Seguridad de la Información para la definición de los datos de prueba que se utilicen para probar mecanismos de acceso a los Activos de Información, las Unidades y Áreas Administrativas deben considerar:

I. El uso de medidas para controlar el acceso cuando la Información de prueba utilizada deba ser protegida conforme a su naturaleza;
II. Los datos utilizados en las pruebas se borren inmediatamente después de concluida y aceptada la prueba, y
III. Las demás que determine la Unidad o Área Administrativa competente conforme a la naturaleza de la Información utilizada en la prueba de que se trate.

CAPÍTULO VII,
INTERRELACIÓN CON LOS PROVEEDORES.

Sección I,
Seguridad de la Información en la interrelación con proveedores.

Artículos 36.- Las Unidades y Áreas Administrativas que celebren contratos con prestadores de servicios, para mantener la Seguridad de la Información deben considerar:

I. La identificación del personal del prestador de servicios que debe acceder a los Activos de Información del Instituto;
II. Establecer los permisos de acceso a los Activos de Información que se permitirá al personal del prestador de servicios;
III. Que se apliquen las medidas de Seguridad de la Información definidas a los Activos de Información;
IV. Definir las obligaciones aplicables a los prestadores de servicios para mantener la Seguridad de la Información del Instituto, y
V. Las demás que resulten necesarias para resguardar la Seguridad de la Información a juicio de las Unidades y Áreas Administrativas competentes atendiendo a su naturaleza.

Artículo 37.- Las Unidades y Áreas Administrativas deben considerar que se incluyan al menos las siguientes especificaciones relacionadas con la Seguridad de la Información en los contratos de prestación de servicios:

I. La descripción de la Información que el Instituto debe proporcionar y la forma de entrega de ésta;
II. Los requisitos legales aplicables para mantener la Seguridad de la Información;

III. Las condiciones de uso de la Información provista por el Instituto a el prestador de los servicios;

IV. El personal del prestador los servicios que está autorizado para recibir Información del Instituto, así como los cambios que realice el mismo;

V. El derecho del Instituto de revisar los procesos relacionados con los servicios contratados, y

VI. Las demás que resulten necesarias para resguardar la Seguridad de la Información a juicio de las Unidades y Áreas Administrativas competentes atendiendo a su naturaleza.

Sección II,
Gestión de la Prestación del Servicio de Aprovisionamiento.

Artículo 38.- En las acciones de revisión y seguimiento de los servicios contratados, las Unidades y Áreas Administrativas deben considerar al menos lo siguiente en materia de Seguridad de la Información:

I. Que se cubran las especificaciones solicitadas para mantener la Confidencialidad, Integridad y Disponibilidad de la Información;

II. Que se proporcione Información sobre los Incidentes de Seguridad de la Información que hayan ocurrido;

III. Que el prestador de servicios conserva la capacidad para cumplir con los requerimientos de Seguridad de la Información solicitados;

IV. Que se atiendan los Criterios que sean emitidos por el Comité, y

V. Las demás que resulten necesarias para resguardar la Seguridad de la Información a juicio de las Unidades y Áreas Administrativas competentes atendiendo a su naturaleza.

CAPÍTULO VIII,
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DE LAS OPERACIONES.

Sección I,
Continuidad de la Seguridad de la Información.

Artículo 39.- En la elaboración de documentos orientados a la continuidad de las operaciones, recuperación de desastres y de contingencia, las Unidades y Áreas Administrativas deben considerar medidas técnicas y organizativas que contribuyan a preservar la Confidencialidad, Integridad y Disponibilidad de la Información.

Artículo 40.- Las Unidades y Áreas Administrativas deberán realizar acciones periódicas orientadas a comprobar la efectividad de las medidas técnicas y organizativas de Seguridad de la Información que adopten en cumplimiento a los Lineamientos.

Sección II,
Redundancia.

Artículo 41.- En lo concerniente a las acciones para dotar de redundancia a los servicios que sean base para el desarrollo de los procesos institucionales relacionados con Activos de Información, el Comité acordará los procesos y proyectos institucionales sobre los que se incluirán medidas para satisfacer los requisitos de Disponibilidad en la Información, en complemento de aquéllas que determinen las Unidades y Áreas Administrativas responsables de los servicios de que se trate, en ejercicio de sus atribuciones y funciones.

INTERPRETACIÓN

Artículo 42.- Corresponde al titular de la Dirección General de Integración, Análisis e Investigación la interpretación de los Lineamientos para efectos administrativos.

Corresponderá al Comité del Sistema de Seguridad de la Información resolver los casos no previstos por los Lineamientos.

TRANSITORIOS

PRIMERO.- Los Lineamientos entrarán en vigor al día siguiente de su publicación en la Normateca Interna del Instituto.

SEGUNDO.- El Comité del Sistema de Seguridad de la Información contará con 180 días hábiles para la aprobación del Listado de Activos de Información del INEGI.

TERCERO.- Las Unidades Administrativas del instituto contarán con un año de calendario a partir de la entrada en vigor de este instrumento para adecuar la normatividad que en su ámbito de competencia deban emitir en atención a lo dispuesto por los Lineamientos.

El presente documento fue aprobado en la Sesión Ordinaria 02 2015 del Comité del Sistema de Seguridad de la Información, celebrada el día 30 de julio de 2015, mediante Acuerdo CSSI-002/ORD-2/2015.

Última hoja de los Lineamientos para el fortalecimiento de la Seguridad de la Información en los procesos y servicios institucionales, el cual se hace constar de 17 fojas útiles y fue publicado en la Normateca Interna del Instituto con fecha 07 de agosto de 2015.