GUÍA DE SEGURIDAD DE LA INFORMACIÓN ESTADÍSTICA Y GEOGRÁFICA

DIRECCIÓN GENERAL DE INTEGRACIÓN, ANÁLISIS E INVESTIGACIÓN

Septiembre, 2021
Aguascalientes, Aguascalientes

ÍNDICE

Introducción 3

1. Actualización y autorización de inventarios 4

2. Identificación de disposiciones normativas en materia de Seguridad de la información en las que se establezcan obligaciones a cumplir 7

3. Identificación de Riesgos de seguridad de la información 9

4. Lista de requerimientos en materia de Seguridad de la información 12

5. Elementos para definir el procedimiento de asignación, modificación y eliminación de permisos 13

6. Requerimiento de Respaldos 15

7. Verificación de implementación de Controles de seguridad de la información 17

8. Revisión de las bitácoras de los accesos a las bases de datos y aplicaciones informáticas 19

9. ANEXOS 20

Lista de anexos 20

ANEXO 1. FORMATO DE AUTORIZACIÓN DE INVENTARIOS 21

ANEXO 2. FORMATO DE INFORME DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN 23

ANEXO 3. FORMATO DE INFORME ANUAL DE CONTROLES E INCIDENTES EN CADA PROGRAMA DE INFORMACIÓN 27

ANEXO 4. FORMATO LISTA DE REQUERIMIENTOS EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN 29

ANEXO 5. FORMATO LISTA DE USUARIOS Y PERMISOS 31

ANEXO 6. FORMATO PLAN DE RESPALDOS 33

ANEXO 7. FORMATO DE VERIFICACIÓN DE CONTROLES 37

ANEXO 8. FORMATO DE INFORME DE VERIFICACIÓN DE CONTROLES 40

ANEXO 9. FORMATO PARA REVISIÓN DE BITÁCORAS 42

Introducción

La Guía de Seguridad de la Información Estadística y Geográfica (Guía) se deriva de la Política para la Seguridad de la Información Estadística y Geográfica del Instituto Nacional de Estadística y Geografía (Política), en cumplimiento a lo establecido en la política Tercera, inciso a), en la que se establece que el Responsable de Seguridad de la Información es la persona servidor público titular de la Dirección General de Integración, Análisis e Investigación, en términos de lo establecido en el Reglamento Interior del Instituto Nacional de Estadística y Geografía, con atribuciones para aprobar los documentos auxiliares que faciliten la instrumentación de las disposiciones normativas en la materia.

La Guía es parte de las acciones que institucionalmente se emprenden para estandarizar las prácticas de Seguridad de la información, facilitar la implementación del marco regulatorio en la materia en el Instituto Nacional de Estadística y Geografía (INEGI), y en conjunto con la Política y los Lineamientos de Seguridad de la Información Estadística y Geográfica del INEGI (Lineamientos) crear las condiciones para el fortalecimiento y mejora continua de la Seguridad de la información que permita contribuir a la construcción de un ecosistema de datos gobernado y seguro que favorezca el logro de los objetivos institucionales.

El diseño de la Guía cubre las directrices establecidas en la Política y los Lineamientos para facilitar el desarrollo de las actividades de la gestión de la Seguridad de la información, las correspondientes a la implementación de controles transversales y específicos en las Fases señaladas en la Norma Técnica del Proceso de Producción de Información Estadística y Geográfica para el INEGI, conforme a las características de la información y las necesidades de protección de ésta, de tal forma que existe una serie de controles aplicables de manera transversal a todo el proceso de producción y otros controles que son necesarios de manera exclusiva en alguna Fase, situación que permite fortalecer la Seguridad de la información de manera sistémica.

La Guía 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 manera inherente en el proceso de producción de información.

En el tiempo y acorde a las necesidades institucionales, esta Guía se actualizará para que mantenga su vigencia y utilidad frente a los riesgos que derivan de los cambios en las formas de trabajar y de los avances tecnológicos, así como de la actualización de la regulación en la materia.

1. ACTUALIZACIÓN Y AUTORIZACIÓN DE INVENTARIOS

A continuación se proporcionan elementos auxiliares para llevar a cabo la actualización y autorización de los inventarios de seguridad de la información señalados en las políticas Décima Primera y Décima Quinta, inciso a), de la Política, y de los artículos 4, 5, 8, 9, 11, 12, 14, 15, 16 y 18, de los Lineamientos.

Se requiere la participación de las siguientes personas servidores públicos: Titular de la Unidad Administrativa, Enlace de Seguridad de la información, Responsable del activo de información, Responsable de Área de Acceso Restringido y Vocal de la Unidad Administrativa.

Herramientas y Recursos

1. Sistema de inventarios de seguridad de la información disponible en la red interna del Instituto en el vínculo siguiente: https://inventariosi.inegi.org.mx/listadosssi/InicioSesion.aspx. Para conectarse fuera de la red interna es necesario contar con una conexión VPN (Virtual Private Network).
2. Lista de Programas de Información disponible en el Sistema de inventarios de seguridad de la información.
3. Lista de Responsables de las Fases de los Programas de Información que corresponden a la Unidad Administrativa de su adscripción.

Términos y ejemplos involucrados

Activo de información

Por ejemplo, la Base de datos generada en la fase de captación, el conjunto de datos vectoriales de información topográfica o el Sistema Informático de Administración de Inventarios para la captación o análisis de la información.

Área de acceso restringido

Por ejemplo, el espacio físico donde se resguardan los cuestionarios.

Redundancia tecnológica

Por ejemplo, los servidores espejo que contienen una réplica exacta del servidor primario, fuentes de energía eléctrica adicionales como una fuente de alimentación interrumpible, mejor conocidas como UPS (uninterruptible power supply).

Para facilitar la actualización y autorización de los inventarios

1. La designación del Responsable del activo de información y del Responsable del Área de Acceso Restringido, así como del Custodio, por parte del Responsable de la Fase (Directores de Área en el caso de las Unidades Administrativas Transversales) y del Responsable del activo de información, respectivamente se da en cumplimiento de las funciones que de manera inherente tiene la persona servidor público en cuanto al cargo que ocupa y para efectos de Seguridad de la Información, se reconoce que el registro de los datos en el Sistema de inventarios de seguridad de la información corresponden a las designaciones señaladas en las políticas Tercera, incisos k), l) y m), y Décima cuarta, inciso c).

2. El Enlace de Seguridad de la información en cumplimiento a lo dispuesto en el artículo 11, fracción I de los Lineamientos, la política Décima Primera, inciso a), con el fin de facilitar la coordinación de la integración de los inventarios, deberá contar con permisos en el Sistema de inventarios de seguridad de la información sobre los perfiles de usuario correspondientes a su adscripción.

3. Para dar cumplimiento a lo señalado en la política Décima Primera, inciso a), es conveniente tener en cuenta instrumentos programáticos como son: lista de los Programas de Información, proyectos informáticos y programas de trabajo, ya que a partir de ellos se pueden identificar las modificaciones necesarias.

4. Dado que para la identificación de Áreas de acceso restringido y requerimientos de Redundancia tecnológica se requiere previamente tener identificados los Activos de información críticos, es conveniente que la actualización de Inventarios se realice en el siguiente orden:

   a) Primero: Inventario de Activos de información.

   b) Segundo: Inventario de Áreas de acceso restringido.

   c) Tercero: Inventario de Requerimientos de Redundancia Tecnológica.

5. Para facilitar la identificación de posibles Activos de información, se debe tomar como base el Catálogo señalado en el artículo 6 de los Lineamientos y contrastarlo con lo dispuesto en los artículos 12, 15, 19, 23, 26, 29, 33 y 36 de la Norma Técnica del Proceso de Producción de Información Estadística y Geográfica.

6. El registro y calificación de los Activos de información corresponde a la Unidad Administrativa responsable del Programa de Información o de la Unidad Administrativa transversal responsable de la información que se almacena y procesa en los Activos de información.

7. Para el registro de Áreas de acceso restringido se debe considerar que, en el Inventario estén las que contengan los Activos de información calificados con nivel ALTO en Confidencialidad o Integridad.
8. Para la autorización anual de los inventarios por parte del Titular de la Unidad Administrativa productora o transversal se requiere que cada Enlace de seguridad de la información notifique vía correo electrónico al Vocal la conclusión de la actualización de los inventarios correspondientes a su adscripción, con el fin de que éste último tenga todos los elementos para gestionar la autorización.
9. En la elaboración del oficio referido en los artículos 4 y 5 de los Lineamientos, se deberá considerar cumplir con los elementos de contenido que establece el ANEXO 1. FORMATO DE AUTORIZACIÓN DE INVENTARIOS.

Lista de evidencias y productos que se deben generar.

1. Inventario de Activos de información.
2. Inventario de Áreas de acceso restringido.
3. Inventario de Requerimientos de Redundancia Tecnológica.
4. Oficio de autorización de los inventarios.

2. IDENTIFICACIÓN DE DISPOSICIONES NORMATIVAS EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN EN LAS QUE SE ESTABLEZCAN OBLIGACIONES A CUMPLIR

A continuación se proporcionan elementos auxiliares para orientar en la identificación de las obligaciones que se tienen que cumplir en materia de Seguridad de la información en el desarrollo de Programas de Información señaladas en la política Vigésima Octava, de la Política, y del artículo 39, de los Lineamientos.

En este apartado se requiere de la participación de las siguientes personas servidores públicos: Actor del Rol Responsable de la Fase de Diseño y Enlace de Seguridad de la información.

1. Para facilitar la identificación de disposiciones normativas en materia de Seguridad de la información en las que se establezcan obligaciones a cumplir se debe considerar lo siguiente:
   a) La temática de la información a generar.
   b) La procedencia y naturaleza de los datos.
   c) Las obligaciones establecidas en las disposiciones normativas y administrativas aplicables en la materia.
2. Se debe considerar una obligación en materia de Seguridad de la información cuando se regulan aspectos para:
   a) Mantener la Confidencialidad, cuando la información sólo es revelada a individuos o procesos autorizados.
   b) Mantener la Integridad, cuando la información se encuentre completa y sin alteraciones.
   c) Mantener la Disponibilidad, cuando la información permanece accesible para su uso cuando lo requieran las personas servidores públicos o procesos autorizados.
   d) Sancionar la pérdida o afectación de la Confidencialidad, Integridad o Disponibilidad.

3. En las disposiciones normativas seleccionadas a partir de lo referido en el presente apartado, en específico en el numeral 1, así como identificar las obligaciones conforme a lo que se indica en el numeral 2 anterior, y registrar en el Documento de Detección de Necesidades señalado en el capítulo II de la Norma Técnica del Proceso de Producción de Información Estadística y Geográfica, al menos, la información siguiente:

a) Nombre completo de la disposición normativa, fecha de publicación y fecha de entrada en vigor.

b) Sección del documento, artículo o numeral de donde se deriva la obligación.

c) Obligación aplicable.

d) Control de seguridad a través del que se cumplirá la obligación.

Evidencia generada

1. Documento de Detección de Necesidades con la información señalada en el numeral 3 del presente apartado.

3. IDENTIFICACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

A continuación se proporcionan elementos auxiliares para orientar en la identificación de los Riesgos de seguridad de la información señalada en las políticas Vigésima Tercera, Vigésima Novena, inciso a) y Trigésima séptima, inciso a), de la Política, y de los artículos 40 fracción I, inciso a), y 56 fracción I, de los Lineamientos.

Se requiere de la participación de las siguientes personas servidores públicos: Actor del Rol Responsable de la Fase, Enlace Informático, Responsable del proceso y personas servidores públicos titulares de las Direcciones de Área en las Unidades Administrativas transversales.

Herramientas

1. Metodología para la Administración de Riesgos en el INEGI: disponible en la Normateca https://sc.inegi.org.mx/repositorioNormateca/Oci_27Nov14.pdf
2. Formato Matriz de Administración de Riesgos: disponible en la Normateca http://sc.inegi.org.mx/repositorioNormateca/Ax_10Mar15.xlsx

Términos y ejemplos involucrados

Riesgo de seguridad de la información

> Por ejemplo, cualquier medio de almacenamiento donde se encuentren los Activos de información es susceptible de sufrir un daño y como consecuencia ocasionar que la información se borre o se pierda. Independientemente de los cuidados que se tengan, la posibilidad siempre existirá y dependerá de las condiciones en las que se encuentre el medio de almacenamiento, así como de las conductas de las personas servidores públicos que lo usen.

Para facilitar la identificación de Riesgos de seguridad de la información

1. Usar el formato de Matriz de Administración de Riesgos dispuesto por la Dirección General Adjunta de Apoyo Normativo y Administración de Riesgos.

2. En la elaboración de la Matriz de Administración de Riesgos considerar los posibles riesgos de las 5 categorías generales que se describen en la tabla siguiente, ya que en ella se consideran las afectaciones a los 3 atributos de Seguridad de la Información:

Categoría general de riesgos de Seguridad de la información	Descripción	Atributo afectado
Acceso no autorizado	Personas o sistemas acceden sin autorización a la información.	Confidencialidad
Exposición de información confidencial	Información confidencial o de divulgación controlada se expone a personas no autorizadas.	Confidencialidad
Pérdida	La información es borrada, robada o destruida de manera que no es posible recuperarla.	Integridad
Alteración	La información es modificada sin autorización.	Integridad
Falta de acceso	No es posible acceder a la información por las personas o sistemas autorizados cuando éstos lo necesitan.	Disponibilidad

3. Los posibles riesgos y las causas relacionadas con los mismos dependerán del contexto de cada programa de información.

Ejemplo de Matriz de Administración de Riesgos:

Unidad administrativa: 0
Nombre del proceso: 0
Objetivo: 0
Alcance: 0%

Análisis de riesgos					
No.	Etapa	Grupo	Descripción	Riesgo	Causa
1	Captación	Seguridad de la información	Dispositivo móvil	Alteración de la información	Robo del dispositivo
2	Procesamiento	Seguridad de la información	Cuestionarios impresos	Acceso no autorizado	Personal ajeno al proceso que ingresa al lugar donde se resguardan los cuestionarios
3	Captación	Seguridad de la información	Dispositivo móvil	Divulgación de información confidencial	Obtener un beneficio personal o a favor de terceros
4	Procesamiento	Seguridad de la información	Servidor	Falta de acceso	No es posibles acceder al lugar donde se resguarda la información en el servidor
5	Transversal	Seguridad de la información	Bases de datos en el servidor	Pérdida de información	Fallas en infraestructura o sistemas informáticos

En el anterior ejemplo se consideran las 5 categorías generales a manera ilustrativa. Para capturar la información del resto de las columnas, seguir las indicaciones de la Metodología e instructivo del formato de la Matriz de Administración de Riesgos.

Evidencia generada

1. Matriz de Administración de Riesgos requisitada.

4. LISTA DE REQUERIMIENTOS EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

A continuación se proporcionan elementos auxiliares para integrar la Lista de requerimientos en materia de Seguridad de la información señalada en la política Trigésima, inciso a), de la Política, y de los artículos 42, 43 y 56, fracción II, de los Lineamientos.

Se requiere de la participación de las siguientes personas servidores públicos: Actor del Rol Responsable de la Fase y titulares de las Direcciones de Área en las Unidades Administrativas transversales.

Términos y ejemplos involucrados

Control de seguridad

Por ejemplo, identificación de requerimientos de respaldos.

Para facilitar la elaboración de la lista de requerimientos en materia de Seguridad de la información se deberá:

1. Tomar en cuenta los controles definidos en la Matriz de Administración de Riesgos (apartado 3 de la presente Guía) y el INFORME ANUAL DE CONTROLES E INCIDENTES EN CADA PROGRAMA DE INFORMACIÓN (anexo 3 de la presente Guía). Para el caso de las Unidades Administrativas productoras, también considerar los controles definidos en el Documento de Detección de Necesidades (apartado 2, numeral 3, inciso d) de la presente Guía).
2. Requisitar el ANEXO 4. FORMATO LISTA DE REQUERIMIENTOS EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN.

Evidencia generada

Formato: lista de requerimientos en materia de Seguridad de la información requisitado.

5. ELEMENTOS PARA DEFINIR EL PROCEDIMIENTO DE ASIGNACIÓN, MODIFICACIÓN Y ELIMINACIÓN DE PERMISOS

A continuación se proporcionan elementos auxiliares para definir el procedimiento de asignación, modificación y eliminación de permisos de acceso a la información, así como el formato para integrar la lista de las personas servidores públicos con permisos asignados, de acuerdo con lo señalado en la política Tercera, inciso k), de la Política, y de los artículos 36 fracción III, 40 fracción III, incisos f) y g), 56 fracciones VIII y IX y 58 fracción III, de los Lineamientos.

Se requiere de la participación de las siguientes personas servidores públicos: Responsable del activo de información, Actor del Rol Responsable de la Fase y personas servidores públicos titulares de las Direcciones de Área en las Unidades Administrativas transversales.

Términos y ejemplos involucrados

Sistema Informático

Por ejemplo, sistema de seguimiento de operativos censales.

Repositorio de información

Por ejemplo, sitio donde se almacenan los informes de actividades del Programa Anual de Estadística y Geografía (PAEG).

En el procedimiento para la asignación, modificación o eliminación de permisos de acceso, el Responsable del activo de información, el Actor del Rol Responsable de la Fase o personas servidores públicos titulares de las Direcciones de Área en las Unidades Administrativas transversales, según corresponda, deben considerar al menos:

a) Definir y autorizar un formato de solicitud de asignación, modificación o eliminación de permisos. Las características y particularidades dependerán del contexto y recursos con los que se cuente.
b) Designar a la persona servidor público que reciba las solicitudes.

1. En la definición del formato de solicitud de asignación, modificación o eliminación de permisos considerar al menos:

   a) Nombre del Activo de información, Sistema Informático o ubicación del Repositorio de información para el que se solicita la asignación, modificación o eliminación de permisos.

   b) Nombre y cargo de la persona servidor público para quien se solicita la asignación, modificación o eliminación de permisos.

   c) Justificación: argumentos que soportan la solicitud.

   d) Vigencia: periodo durante el que se requiere la asignación y en su caso modificación de permisos.

2. Para integrar la lista de las personas servidores públicos que tienen permisos asignados se debe usar como referencia el ANEXO 5. LISTA DE USUARIOS Y PERMISOS.

3. Se deberá guardar en un lugar seguro y preferentemente cifrado la LISTA DE USUARIOS Y PERMISOS a la que se refiere el punto anterior.

Evidencia generada

1. Lista de usuarios y permisos requisitada.

6. REQUERIMIENTO DE RESPALDOS

A continuación se proporcionan elementos auxiliares para la integración de los requerimientos de respaldos señalado en las políticas Vigésima Cuarta, inciso h), Trigésima Séptima, inciso d), y de los artículos 37 y 59, de los Lineamientos.

Se requiere la participación de las siguientes personas servidores públicos: Actor del Rol Responsable de la Fase y personas servidores públicos titulares de las Direcciones de Área en las Unidades Administrativas transversales.

Términos y ejemplos involucrados

Activo de información

Por ejemplo, la Base de datos generada en la fase de captación, el conjunto de datos vectoriales de información topográfica o el Sistema Informático para la captación o análisis de la información.

Respaldo

Por ejemplo, las copias de los archivos que se almacenan en un servidor de archivos distinto al que contiene los datos originales.

Restauración de los respaldos

Por ejemplo, cuando se pierden los archivos y por lo tanto se accede a la copia almacenada en una ubicación distinta para continuar con las operaciones.

Repositorio

Por ejemplo**,** los servidores en donde se almacena la información.

Para facilitar la elaboración del requerimiento de respaldo se debe considerar lo siguiente:

1. Para la especificación de requerimientos de respaldo dentro de la fase, utilizar el ANEXO 6. FORMATO PLAN DE RESPALDOS.
2. El requerimiento de respaldos considera como mínimo a los Activos de información que les aplique de acuerdo con la Lista de Controles mínimos de Seguridad de la Información.
3. Para los casos en los que el Activo de información requiera de un programa o entorno particular para acceder a su contenido, considerar incluirlo como parte del respaldo.

   Por ejemplo, si se respaldan archivos Shapefile (SHP) conviene respaldar una copia del Sistema Informático que permite acceder al contenido de este.

Evidencia generada

1. Formato plan de respaldos de la fase requisitado.

7. VERIFICACIÓN DE IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

A continuación se proporcionan elementos auxiliares para llevar a cabo la verificación de la implementación de los Controles de seguridad a que hacen referencia las políticas Vigésima Cuarta, inciso a), y Trigésima Octava, inciso a), de la Política.

Para el cumplimiento de esta actividad de verificación se requiere de la participación de las siguientes personas servidores públicos: Actor del Rol Responsable de la Fase, Enlace Informático y titulares de las Direcciones de Área en las Unidades Administrativas transversales.

Términos y ejemplos involucrados

Control de seguridad

Por ejemplo, identificación de requerimientos de respaldos.

Control de seguridad de la información del tipo administrativo

Por ejemplo, lista actualizada de personal autorizado, procedimiento para solicitud de permisos, listas de asistencia que acrediten los cursos de capacitación.

Control de seguridad de la información del tipo físico

Por ejemplo, restricción de acceso físico a áreas que contienen Activos de información, resguardo de instrumentos de captación en Áreas de acceso restringido.

Control de seguridad de la información del tipo técnico

Por ejemplo, acceso vía usuario y contraseña, antivirus, respaldos o activación de bitácoras de generación automática.

Así mismo, para facilitar la verificación de implementación de controles de seguridad de la información es necesario considerar que:

1. La verificación de la implementación de los controles no es una auditoría, sino una actividad para supervisar la aplicación de los controles, comprobar su efectividad y mejorar su aplicación.
2. La actividad aplica para la verificación de los controles independientemente de su origen, ya sea que hayan sido identificados a partir de la Matriz de Administración de Riesgos o bien, de otro tipo de ejercicio de planeación o definición de requerimientos.
3. Registrar el resultado de la verificación de cada control en el ANEXO 7. FORMATO DE VERIFICACIÓN DE CONTROLES.
4. Utilizar el ANEXO 8. FORMATO DE INFORME DE VERIFICACIÓN DE CONTROLES.

Evidencia generada

1. Formato de verificación de controles requisitado.
2. Formato de informe de verificación de controles requisitado.

8. REVISIÓN DE LAS BITÁCORAS DE LOS ACCESOS A LAS BASES DE DATOS Y APLICACIONES INFORMÁTICAS

A continuación se proporcionan elementos auxiliares para llevar a cabo la revisión, de las bitácoras electrónicas de los accesos a las bases de datos y aplicaciones informáticas para identificar Eventos de seguridad de la información, señalada en el artículo 48, de los Lineamientos.

Se requiere la participación del Actor del Rol Responsable de la Fase.

Para facilitar la revisión de las bitácoras de los accesos a las bases de datos y aplicaciones informáticas se debe:

Requisitar el ANEXO 9. FORMATO PARA REVISIÓN DE BITÁCORAS para la identificación de Eventos en la revisión de las bitácoras de los accesos a las bases de datos y aplicaciones informáticas.

Evidencia generada

1. Formato para revisión de bitácoras requisitado.

9. ANEXOS

LISTA DE ANEXOS

1. ANEXO 1. FORMATO DE AUTORIZACIÓN DE INVENTARIOS.
2. ANEXO 2. FORMATO DE INFORME DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN.
3. ANEXO 3. FORMATO DE INFORME ANUAL DE CONTROLES E INCIDENTES EN CADA PROGRAMA DE INFORMACIÓN.
4. ANEXO 4. FORMATO LISTA DE REQUERIMIENTOS EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN.
5. ANEXO 5. LISTA DE USUARIOS Y PERMISOS.
6. ANEXO 6. FORMATO PLAN DE RESPALDOS.
7. ANEXO 7. FORMATO DE VERIFICACIÓN DE CONTROLES.
8. ANEXO 8. FORMATO DE INFORME DE VERIFICACIÓN DE CONTROLES.
9. ANEXO 9. FORMATO PARA REVISIÓN DE BITÁCORAS.

ANEXO 1. FORMATO DE AUTORIZACIÓN DE INVENTARIOS

SECRETARIO

Secretario Ejecutivo del Comité de Seguridad y Confidencialidad

Estadística de la Información

P r e s e n t e

Conforme a lo establecido en los artículos 4 y 5 de los *Lineamientos de Seguridad de la Información Estadística y Geográfica del INEGI*, le notifico la actualización y autorización de los inventarios de seguridad de la información correspondientes a esta Unidad Administrativa, mismos que están disponibles en el Sistema de inventarios de seguridad de la información designado por la DGIAI para tal fin.

Atentamente

TITULAR

C.p. Presidente del Comité de Seguridad y Confidencialidad Estadística de la Información.

DSCI, -DGIAI

Enlaces de Seguridad de la Información.

Instructivo del ANEXO 1. FORMATO DE AUTORIZACIÓN DE INVENTARIOS

SECRETARIO: nombre completo del Titular del Secretario Ejecutivo del Comité de Seguridad y Confidencialidad Estadística de la Información.

TITULAR: nombre completo del Titular de la Unidad Administrativa que autoriza los inventarios de la Unidad Administrativa correspondiente.

Presidente: nombre del Titular de la Presidencia del Comité.

DSCI: nombre completo y puesto del Titular o responsable de la Dirección de Seguridad y Confidencialidad de la Información.

Enlaces de Seguridad de la información: nombre (s) completo y puesto (s) del Enlace (s) de la Unidad Administrativa correspondiente.

ANEXO 2. FORMATO DE INFORME DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

Fecha y hora de la notificación	
Unidad Administrativa	
Programa de Información o actividad transversal en la que se presentó el Incidente	
Fase del Proceso de Producción en la que se presentó el Incidente	
ID y Nombre de los Activos de información críticos	
Afectaciones en términos de Confidencialidad, Integridad o Disponibilidad	
Causas	
Impactos	
Acciones implementadas para dar respuesta	
Personal involucrado en la respuesta al Incidente	
Probabilidad de que el Incidente se vuelva a presentar	
Acciones propuestas para disminuir la probabilidad de que el Incidente se vuelva a presentar	
Fecha de elaboración del reporte	

Instructivo del ANEXO 2. FORMATO DE INFORME DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

Fecha y hora de la notificación: se obtiene de la ficha de registro en el Módulo de la Mesa de Ayuda

Por ejemplo, miércoles 18 de noviembre de 2020, 13:15 h.

Unidad Administrativa: nombre de la Unidad Administrativa a la que corresponde el Programa de Información o actividad en la que se presentó el Incidente, puede existir el caso de que haya más de una Unidad Administrativa involucrada.

Por ejemplo, Dirección General de Estadísticas Sociodemográficas, Dirección General de Geografía y Medio Ambiente.

Programa de Información o actividad transversal en la que se presentó el Incidente: nombre del Programa o Programas de Información a los que corresponde la Información que ha sido afectada o en su defecto, el proyecto estadístico o geográfico.

Por ejemplo, Red Nacional de Caminos.

Fase del Proceso de Producción en la que se presentó el Incidente: nombre de la o las Fases a las que corresponden las actividades en las que se manifestó el Incidente. En el caso de que el Incidente no corresponda a un Programa de Información, indicar “no aplica”.

Por ejemplo, captación.

ID y Nombre de los Activos de información críticos: ID y Nombre de los Activos de Información críticos, en el caso de que así haya sido, de lo contrario indicar “no aplica”.

Por ejemplo, ID 12, Base de datos de captura de la Encuesta.

Afectaciones en términos de Confidencialidad, Integridad o Disponibilidad: descripción del daño comprobado en la información.

Por ejemplo, pérdida de la totalidad de la Base de datos central de captura actualizada al 18 de noviembre.

Causas: enumerar y describir las situaciones que causaron el Incidente, los datos se obtienen después de aplicar la técnica de los 5 porqué o alguna herramienta similar.

Por ejemplo, la Base de datos se perdió debido a que el ransomware *Ceber* cifró los datos. El ransomware se instaló en el servidor a través de la computadora infectada de una persona con permisos de acceso. El ransomware ingresó a la red interna del Instituto debido a que un usuario descargó y ejecutó un archivo adjunto a un correo enviado por un remitente desconocido que

simuló ser una institución bancaria. El ransomware se pudo distribuir al interior del Instituto debido a la explotación de una vulnerabilidad en el sistema operativo.

Impactos: enumerar y describir las afectaciones ocasionadas por el Incidente.

Por ejemplo, durante tres días no fue posible transmitir la información a la Base de datos central;

Acciones implementadas para dar respuesta: enumerar y describir las principales acciones para responder al Incidente.

Por ejemplo:

- Aislamiento: desconexión de la red de los equipos identificados.
- Identificación de potenciales equipos infectados para su aislamiento.
- Generación de un nuevo entorno para alojar la Base de datos.
- Recuperación del respaldo inmediato anterior y puesta en producción.
- Análisis y conciliación de la Base de datos respecto de los registros faltantes.

Personal involucrado en la respuesta al Incidente: enumerar el nombre de las personas servidores públicos que participaron en la definición e implementación de la respuesta al Incidente, incluyendo personal interno y externo e indicando su área de adscripción.

Por ejemplo:

- María Morales. Dirección General Adjunta de Apoyo Normativo y Administración de Riesgos. DGA.
- Juan Ramírez. Dirección de Seguridad Informática. CGI.
- Elena Olivares. Dirección de Seguridad y Confidencialidad de la Información. DGIAI.
- Raúl Romo. Dirección de Seguridad y Confidencialidad de la Información. DGIAI.
- Mónica Merino. Oracle.

Probabilidad de que el Incidente se vuelva a presentar: considerar las causas y los factores adicionales que dieron origen al Incidente y con base en esa información elegir entre los siguientes valores: Alta, Media o Baja, e incluir los argumentos que soportan la estimación.

Por ejemplo, media: frecuentemente llegan correos de distintos remitentes con características similares al mensaje que ocasionó la infección.

Acciones propuestas para disminuir la probabilidad de que el Incidente se vuelva a presentar: derivado de las medidas implementadas para dar respuesta y del análisis posterior, enumere las acciones enfocadas para disminuir la probabilidad de que el Incidente se repita.

Por ejemplo:

- Monitoreo e instalación de parches de seguridad en los equipos de cómputo.
- Concientización al personal respecto al correo phishing.

Fecha de elaboración del reporte: día, mes y año en la que se concluye la elaboración del reporte.

ANEXO 3. FORMATO DE INFORME ANUAL DE CONTROLES E INCIDENTES EN CADA PROGRAMA DE INFORMACIÓN

Unidad Administrativa	Periodo de referencia	
Programa de Información		
Activos de información	**Control**	**Incidente**
Fecha de elaboración:		

Instructivo del ANEXO 3. FORMATO DE INFORME ANUAL DE CONTROLES E INCIDENTES EN CADA PROGRAMA DE INFORMACIÓN

Unidad Administrativa: nombre de la Unidad Administrativa a la que corresponde el Programa de Información.

Por ejemplo, Dirección General de Geografía y Medio Ambiente.

Programa de Información: nombre del Programa de Información al que corresponde el Informe.

Por ejemplo, Uso de suelo y vegetación.

Activo de información: extraer del inventario de Activos de información los datos contenidos en el campo “Id” y “nombre del Activo de Información”.

Por ejemplo, 234 Base de datos de la ENSHDU.

Control: enumerar los controles implementados para proteger la información en la ejecución del proceso de producción, ya sea de manera transversal o de manera específica en las fases.

Por ejemplo:

1. Acceso restringido físico a las áreas donde se almacena o procesa información.
2. Acceso restringido a los Repositorios y Sistemas Informáticos.
3. Cifrado de información en el almacenamiento y transmisión de la información.
4. (..)

Incidentes: si no se presentaron incidentes, escribir *“No se presentaron Incidentes de seguridad de la información”*. De lo contrario, enumerar los Incidentes que se hayan presentado, incluyendo la fecha y la afectación:

Por ejemplo, 18/11/2020. Pérdida de la totalidad de la Base de datos central de captura actualizada al 18 de noviembre.

Fecha de elaboración del reporte: fecha en formato dd/mm/aaaa en la que se concluye la elaboración del reporte.

ANEXO 4. FORMATO LISTA DE REQUERIMIENTOS EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

Unidad Administrativa:	
Programa de Información:	
Fase:	
Actor del Rol Responsable de la Fase:	
Fecha de última revisión:	

Núm.	Control o característica.	Activo de información.
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		

Instructivo del ANEXO 4. FORMATO LISTA DE REQUERIMIENTOS EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

Unidad Administrativa: nombre de la Unidad Administrativa responsable del Programa de Información al que corresponden los controles.

Programa de Información: nombre del Programa de Información al que corresponden los controles. En el caso de las Unidades Administrativas transversales ingresar el nombre del proyecto.

Fase: nombre de la fase a la que corresponden los controles. No aplica para el caso de las Unidades Administrativas transversales.

Actor del Rol Responsable de la Fase: nombre del Actor del Rol Responsable de la Fase. Para el caso de las Unidades Administrativas transversales ingresar el nombre de la persona servidor público titular de la dirección de área.

Fecha última revisión: día, mes y año en la que se realizó la última revisión o modificación de la lista.

Núm.: identificador consecutivo de cada control o característica.

Control o característica: tomar en cuenta los controles definidos en la Matriz de Administración de Riesgos, el anexo 3 de la presente Guía, para el caso de las Unidades Administrativas productoras, también considerar los controles definidos en la sección 3 de esta Guía.

Activo de Información: ID y nombre del Activo de información al que le resulta aplicable el control.

ANEXO 5. FORMATO LISTA DE USUARIOS Y PERMISOS

Unidad Administrativa:	
Activo o Activos de información:	[Incluir el ID y el nombre del activo]
Fecha de última revisión:	

Núm.	Nombre o cuenta de usuario	Permisos asignados (marcar con una "X" los permisos asignados)		
		Lectura	Escritura	Administración
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

Instructivo del ANEXO 5. FORMATO LISTA DE USUARIOS Y PERMISOS

Unidad Administrativa: nombre de la Unidad Administrativa a la que corresponde el Programa de Información o actividad en la que se presentó el Incidente, puede incorporarse el caso de que haya más de una Unidad Administrativa involucrada.

Por ejemplo, Dirección General de Estadísticas Económicas.

Activo o Activos de información: la lista puede realizarse a nivel individual o por grupo de Activos de información si es que comparten los mismos permisos. Para facilitar su identificación incluir el ID que le corresponde según el Inventario de Activos de información y su nombre.

Fecha última revisión: día, mes y año en la que se realizó la última revisión o modificación de la tabla de permisos.

Núm.: identificador consecutivo de cada nombre o cuenta de usuario.

Nombre o cuenta de usuario: anotar el nombre de la persona a la que se están asignando los permisos, cuando corresponda a una cuenta especial o asignada a alguna aplicación, anotar el nombre de usuario; en caso de ser un usuario externo después del nombre entre paréntesis poner el origen (nombre de la empresa pública o privada o si es por cuenta propia), precedido de un “punto y coma” el objetivo del permiso (consultoría, servicio social, etcétera).

Permisos asignados: marcar con una “X” en la columna que corresponde al permiso asignado, de lo contrario marcar con doble guion medio “—“.

Lectura: quien tiene este permiso puede acceder a la información, pero no le será posible hacer modificaciones o eliminaciones.

Escritura: quien tiene este permiso, puede acceder a la información, modificarla e inclusive borrarla.

Administración: quien tiene este permiso, puede acceder a la información, modificarla, borrarla y proporcionar acceso a la misma a otras personas servidores públicos. Según el sistema operativo o la aplicación de la que se trate, puede ejecutar otro tipo de tareas específicas.

ANEXO 6. FORMATO PLAN DE RESPALDOS

Unidad Administrativa:	
Programa de Información:	
Fase:	
Actor del Rol Responsable de la Fase:	
Fecha de última revisión:	

Activo o Activos de información	Equipo o ruta de almacenamiento	Tipo de respaldo	Frecuencia	Periodo de conservación

Lista del personal autorizado para acceder y recuperar los respaldos:	
Medios de almacenamiento donde se ubica el respaldo:	

Instructivo del ANEXO 6. FORMATO PLAN DE RESPALDOS

Unidad Administrativa: nombre de la Unidad Administrativa a la que corresponde el Programa de Información o actividad en la que corresponden los Activos de información a respaldar.

Programa de Información: nombre del Programa de Información al que corresponden los Activos de información a respaldar.

Fase: nombre de la fase a la que corresponden los Activos de información a respaldar.

Actor del Rol Responsable de la Fase: nombre del Actor del Rol Responsable de la Fase.

Fecha última revisión: día, mes y año en la que se realizó la última revisión o modificación del plan de respaldos.

Activo o Activos de información: ID y nombre del Activo información que se va a respaldar, puede incluirse a más de un Activo de información cuando se encuentren almacenados en la misma carpeta y compartan los mismos requerimientos de respaldos.

Cuando se trate de Información o programas de software especializados que sean necesarios para la recuperación de los Activos de información críticos, escribir el nombre del archivo o programa.

Equipo o ruta de almacenamiento: nombre del servidor o dirección IP, ruta de carpetas en donde se encuentra el Activo de información y desde donde se realizará la copia.

Por ejemplo, \\w-appintrafilex9\OficinaCDRT\Informes

Tipo de respaldo: indicar según corresponda con la siguiente lista:

1. Escribir **"Total":** cuando se realiza una copia de todos los archivos y directorios. Este proceso puede durar horas dependiendo del tamaño de los archivos o directorios a copiar, por lo que este proceso normalmente se ejecuta la primera vez que se realiza el respaldo o en periodos de tiempo como cada año, o bien, para cuando se trata de versiones finales.
2. Escribir **"Diferencial":** cuando únicamente se requiere copiar los archivos y directorios que han sido creados y/o modificados desde la última copia completa.
3. Escribir **"Incremental":** cuando únicamente se requiere copiar los archivos y registros creados o modificados desde el último respaldo, ya sea de una copia completa o incremental, reduciendo de este modo los archivos a copiar y el tiempo empleado en el proceso.

Frecuencia: indicar según corresponda con la siguiente lista:

Escribir **"Diario"** cuando se requiera que el respaldo se realice una vez al día, también indicar la hora en la que se requiere que se realice el respaldo.

Por ejemplo, diario a las 17:00 h

Escribir **"Semanal"** cuando se requiera que el respaldo se realice una vez a la semana, también indicar el día de la semana y la hora en la que se requiere que se realice el respaldo.

Por ejemplo, semanal, cada viernes a las 17:00 h

Escribir **"Mensual"** cuando se requiera que el respaldo se realice una vez al mes, también indicar el día de cada mes y la hora en la que se requiere que se realice el respaldo.

Por ejemplo, mensual, cada cuarto viernes de cada mes a las 17:00 h

Escribir **"Anual"** cuando se requiera que el respaldo se realice una vez al año, también indicar el mes, día y hora en la que se requiere que se realice el respaldo.

Por ejemplo, Anual, cada cuarto viernes de diciembre a las 17:00 h

Escribir **"Especial"**: cuando el respaldo no entre en ninguno de los casos anteriores, cuando sea así, indicar aspectos que permitan identificar la necesidad en términos de cada cuando, en qué día y qué hora se debe realizar el respaldo.

Periodo de conservación: indicar el periodo que se requiere que se mantenga el respaldo, puede ser en términos de días, semanas, meses o años.

Lista del personal autorizado para acceder y recuperar los respaldos: personal que ha sido autorizado por el Responsable del activo de información para acceder o recuperar los respaldos.

Medios de almacenamiento donde se ubica el respaldo: cuando el respaldo se almacene e los servicios administrados por la Coordinación General de Informática anotar "CGI" En caso contrario, la dirección, nombre, ubicación u otro dato de identificación del repositorio que contiene los respaldos.

ANEXO 7. FORMATO DE VERIFICACIÓN DE CONTROLES

Programa de Información:								
Fecha:								
Núm.	**Control**	**Responsable**	**Fase en lo que aplica**	**Tipo**	**Cantidad de Instancias a las que aplica**	**Estatus del Control**	**Descripción de la evidencia**	**¿Ayudó o mitigar el riesgo?**
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								

Instructivo del ANEXO 7. FORMATO DE VERIFICACIÓN DE CONTROLES

Programa de Información: nombre del Programa de Información al que corresponde el Informe.

Por ejemplo, Uso de suelo y vegetación.

Fecha: día, mes y año en la que finaliza la verificación de controles.

Control: el nombre del control se obtiene del instrumento que corresponda en donde se definió la obligatoriedad de implementar los controles.

Por ejemplo, acceso vía usuario y contraseña a Sistemas Informáticos.

Responsable: nombre de la persona servidor público que implementa el control.

Fase en la que se aplica: cuando el control se aplique en todo el proceso escribir *"transversal"* cuando sea en una fase en particular escribir el nombre de la fase.

Tipo: elegir según corresponda:

Control de seguridad de la información del tipo administrativo: procedimientos, formatos de control, acciones de comunicación, capacitación o concientización.

Por ejemplo, lista actualizada de personal autorizado, procedimiento para solicitud de permisos, listas de asistencia que acrediten los cursos de capacitación, Notas, Oficios y correos electrónicos donde se comunique alguna directriz.

Control de seguridad de la información del tipo físico: conjunto de acciones y mecanismos para proteger el entorno físico donde se llevan a cabo las operaciones con Activos de información.

Por ejemplo, restricción de acceso físico a áreas que contienen Activos de información, resguardo de Instrumentos de captación en Áreas de acceso restringido.

Control de seguridad de la información del tipo técnico: conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para la protección de los Activos de información.

Por ejemplo, acceso vía usuario y contraseña, Antivirus, Respaldos o activación de bitácoras de generación automática.

Cantidad de instancias a las que aplica: escribir con número la cantidad de instancias a las que aplica el control.

Estatus del control: seleccionar según corresponda:

Implementado: el control forma parte de los procedimientos y herramientas que se usan en el desarrollo de las actividades.

Listo para implementarse: para el caso de los controles definidos para atenuar el impacto derivado de la materialización de un Riesgo, el personal lo identifica, conoce las condiciones en las que hay que usarse, así como el procedimiento.

Sin implementar: cuando no se encuentre evidencia de que el control forma parte de los procedimientos y herramientas que se usan en el desarrollo de las actividades.

Descartado: cuando se encuentre evidencias de que el control afecta la operación o bien, cuando las condiciones de las actividades hayan cambiado y el control ya no sea necesario.

Descripción de la evidencia: cuando el control tiene el estatus de implementado o listo para implementarse, incorporar la descripción de evidencia según corresponda.

Evidencias que soportan la implementación de control de tipo administrativo: obtener copia de la documentación que acredite la implementación.

Evidencias que soportan la implementación de control de tipo físico: asistir de manera física y documentar a través de fotografías la operación de control.

Evidencias que soportan la implementación de control de tipo técnico: operar la funcionalidad técnica y tomar fotografía, captura de pantalla, reporte de aplicación de control u obtener una copia de las bitácoras automáticas que den evidencia de la operación.

Cuando en la verificación se identifique que algún control ha sido descartado, incluir la descripción de la evidencia que soporta tal situación.

Cuando en la verificación se identifique que algún control no ha sido implementado, no es necesario proporcionar información en esta columna.

¿Ayudó a mitigar el Riesgo? Aplica únicamente para los casos en los que el control se encuentra implementado, como respuesta colocar “sí” o “no”.

ANEXO 8. FORMATO DE INFORME DE VERIFICACIÓN DE CONTROLES

Unidad Administrativa:	**Fecha de elaboración**
Programa de Información:	
Total de controles objeto de verificación:	

Controles administrativos	**Controles físicos**	**Controles técnicos.**
Controles administrativos implementados	**Controles físicos implementados**	**Controles técnicos implementados**

Conclusiones

Instructivo del ANEXO 8. FORMATO DE INFORME DE VERIFICACIÓN DE CONTROLES

Unidad Administrativa: nombre de la Unidad Administrativa a la que corresponde el Programa de Información o actividad sobre la que se hace la verificación.

Por ejemplo, Dirección General de Estadísticas Económicas.

Fecha de elaboración del reporte: día, mes y año en la que se concluye la elaboración del informe.

Programa de Información: nombre del Programa de Información al que corresponde el Informe.

Por ejemplo, Uso de suelo y vegetación.

Total de controles objeto de verificación: anotar el total de los controles que se verificaron según el ANEXO 7. FORMATO DE VERIFICACIÓN DE CONTROLES.

Controles administrativos: anotar el total de controles del tipo administrativo que se verificaron según el ANEXO 7. FORMATO DE VERIFICACIÓN DE CONTROLES.

Controles físicos: anotar el total de controles del tipo físico que se verificaron según el ANEXO 7. FORMATO DE VERIFICACIÓN DE CONTROLES.

Controles técnicos: anotar el total de controles del tipo técnicos que se verificaron según el ANEXO 7. FORMATO DE VERIFICACIÓN DE CONTROLES.

Controles administrativos implementados: anotar el total de controles del tipo administrativo que en el ANEXO 7. FORMATO DE VERIFICACIÓN DE CONTROLES tienen el estatus de implementado.

Controles físicos implementados: anotar el total de controles del tipo físico que en el ANEXO 7. FORMATO DE VERIFICACIÓN DE CONTROLES tienen el estatus de implementado.

Controles técnicos implementados: anotar el total de controles del tipo técnicos que en el ANEXO 7. FORMATO DE VERIFICACIÓN DE CONTROLES tienen el estatus de implementado.

Conclusiones: redactar un párrafo en el que se dé cuenta de alguna situación que se quiera destacar derivado de la verificación.

ANEXO 9. FORMATO PARA REVISIÓN DE BITÁCORAS

Unidad Administrativa:			
Programa de Información o Actividad Transversal:			
Nombre de quien realiza la revisión			
Base de datos o aplicación informática:	**Fecha de última revisión:**	**Periodo de revisión:**	**Evento identificado**

Instructivo del ANEXO 9. FORMATO PARA REVISIÓN DE BITÁCORAS

Unidad Administrativa: nombre de la Unidad Administrativa a la que corresponde el Programa de Información o actividad en la que corresponden los Activos de información a respaldar.

Programa de Información: nombre del Programa de Información al que corresponden los Activos de información a respaldar.

Base de datos o aplicación informática: nombre y descripción la base de datos a la que corresponden las bitácoras.

Fecha última revisión: día, mes y año en la que se realizó la revisión de las bitácoras.

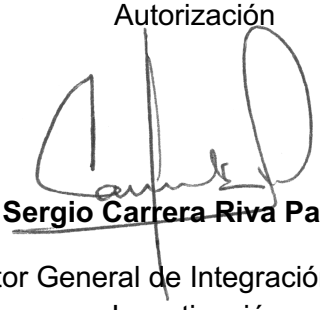
Periodo de revisión: rango de fechas al que corresponde las bitácoras revisadas.

Por ejemplo, del 01/01/2021 al 30/04/2021.

Evento identificado: elegir número según corresponda:

1. **Acceso de usuarios no autorizados.**
2. **Usuarios realizan acciones que no corresponden con el nivel de permiso asignado.**
3. **Acceso, modificación o eliminación de información fuera de horario laboral.**
4. **Exportación de información confidencial o de divulgación controlada.**
5. **Otros:** en el caso de que el evento sea diferente al de las columnas anteriores, describir en formato libre la situación y los impactos potenciales a la seguridad de la información.

Autorización



Sergio Carrera Riva Palacio

Director General de Integración, Análisis e Investigación.

En términos de las atribuciones que le confiere el artículo 29 del Reglamento Interior del Instituto Nacional de Estadística y Geografía, así como la Política Tercera inciso a), de la Política para la Seguridad de la Información Estadística y Geográfica del Instituto Nacional de Estadística y Geografía.