INSTITUTO NACIONAL
DE ESTADÍSTICA Y GEOGRAFÍA

PROTOCOLO INSTITUCIONAL DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

COMITÉ DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN.

JULIO 2015.
Aguascalientes, Aguascalientes.

ÍNDICE

INTRODUCCIÓN 3

A. Disposiciones Generales. 4

B. Notificación de Eventos. 5

C. Evaluación y toma de decisiones en torno a Eventos de Seguridad de la Información. 7

D. Respuesta a Incidentes de Seguridad de la Información. 8

E. Aprendizaje de los Incidentes de Seguridad de la Información. 10

F. INTERPRETACIÓN 11

TRANSITORIOS 11

INTRODUCCIÓN

La identificación, registro, análisis y resolución de los Incidentes de Seguridad de la Información es un aspecto importante para lograr la mejora continua en el Sistema de Seguridad de la Información del Instituto Nacional de Estadística y Geografía, ya que complementa las acciones derivadas de la publicación de las Políticas para la Seguridad de la Información del Instituto Nacional de Estadística y Geografía, así como el desarrollo de Matrices de Administración de Riesgos en el marco del Control Interno; con el fin de mantener la Seguridad de la Información, tanto la de la Gestión Administrativa del Instituto así como la Estadística y Geográfica, ésta última suministrada a la sociedad y al Estado en los términos previstos en el artículo 3 de la Ley del Sistema Nacional de Información Estadística y Geográfica (LSNIEG).

El Protocolo Institucional de Respuesta a Incidentes de Seguridad de la Información (Protocolo) establece las líneas de acción a partir de las cuales deberán atenderse los Incidentes de Seguridad de la Información; comprende desde los medios de comunicación a utilizar para el reporte de los eventos relacionados con la Seguridad de la Información, hasta las acciones a realizar para incorporar el aprendizaje que se genera en la atención de los Incidentes de Seguridad de la Información.

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

PROTOCOLO INSTITUCIONAL DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

A. Disposiciones Generales.

A.1. El presente Protocolo tiene por objeto definir las líneas de acción a partir de las cuales las Unidades y Áreas Administrativas del Instituto, deberán implementar acciones dentro de su ámbito de competencia para identificar, registrar y atender los Incidentes de Seguridad de la Información.

A.2. Las disposiciones del presente Protocolo son de observancia general y obligatoria para las Unidades y Áreas Administrativas del Instituto y los servidores públicos adscritos a las mismas. Corresponde a los Titulares de las Unidades Administrativas implementar y dar cumplimiento en su respectivo ámbito de competencia.

A.3. 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 del presente documento se entenderá por:

1. **Amenaza:** Causa potencial de un Incidente no deseado, que puede provocar daños a un sistema o a la organización;
2. **Aplicación, o Aplicaciones informáticas:** Sistemas informáticos y/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;
3. **Comité:** Comité del Sistema de Seguridad de la Información;
4. **Equipamiento:** Los servidores departamentales, las computadoras de escritorio, computadoras portátiles, impresoras, escáneres y multifuncionales portátiles, entre otros;
5. **Evidencias:** Conjunto de pruebas que dejan vestigio de un Incidente de Seguridad de la Información, sus causas e impactos;
6. **Grupo de Trabajo:** Grupo de servidores públicos que se integra de manera temporal con el objetivo de analizar un Incidente de Seguridad de la Información;

7. **Medios de Almacenamiento:** Es el material físico donde se almacenan los datos;
8. **Mesa de ayuda:** Las Áreas Administrativas que reciben y turnan las solicitudes de soporte técnico de los usuarios de servicios relacionados con TIC;
9. **Prestigio Institucional:** Credibilidad y confianza que la sociedad ha depositado en el Instituto;
10. **Protocolo:** Protocolo Institucional de Respuesta a Incidentes de Seguridad de la Información del Instituto Nacional de Estadística y Geografía, y
11. **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 Instituto o a terceros.

B. Notificación de Eventos.

B.1. Todos los servidores públicos del Instituto están obligados a reportar en términos de lo dispuesto por el Protocolo, cualquiera de los siguientes eventos:

1. Cuando las condiciones del entorno supongan un factor de Riesgo para la Información, los servicios tecnológicos, la operación de los procesos, el uso de los inmuebles;
2. Cuando la información esté expuesta y pueda sufrir algún daño o pueda ser accedida sin autorización;
3. Cuando el funcionamiento de Aplicaciones Informáticas pongan en Riesgo la Confidencialidad, Integridad y Disponibilidad de la Información;
4. Cuando hayan presenciado un daño a la Información;
5. El incumplimiento de políticas o directrices en materia de Seguridad de la Información;
6. El acceso no autorizado a la Información, áreas o instalaciones restringidas;
7. La alteración, pérdida total o parcial de la Información, y
8. Cualquier otra circunstancia que a juicio de los servidores públicos comprometa la Seguridad de la Información.

B.2. La notificación de los eventos descritos en el punto anterior se podrá realizar mediante:

1. Llamada telefónica a la Mesa de Ayuda, en términos del punto B.3. del Protocolo;
2. Registro del reporte en la sección de Mesa de Ayuda en la Intranet del Instituto;

3. Envío de correo electrónico a la cuenta: *mesa.ayuda@inegi.org.mx*, y

4. De manera personal, notificando al Enlace de Seguridad de la Información de su respectiva Unidad Administrativa, al Enlace de Informática en las Direcciones Regionales así como a las Subdirecciones de Informática en las Coordinaciones Estatales.

B.3. Para el reporte telefónico, se realizará a través del esquema de Mesa de Ayuda, a la extensión 5000 en la Ciudad de Aguascalientes, al 01 800 463 4402 a nivel nacional, así como en cada una de las extensiones locales de cada Dirección Regional del Instituto.

B.4. Corresponde a la Dirección General de Integración Análisis e Investigación, de manera conjunta con la Dirección General Adjunta de Informática, definir las características, desarrollar y poner en marcha un Módulo para el Registro de las Notificaciones de Eventos, dentro de la plataforma de la Mesa de Ayuda, el cual deberá considerar la captación de las siguientes variables:

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

2. Sitio donde tuvo lugar el evento (Entidad Federativa, Municipio, edificio y oficina);

3. Unidad Administrativa relacionada o posiblemente impactada por el evento;

4. Procesos, proyectos, servicios y productos o Información afectados;

5. Servidor público o personal que notifica el evento;

6. Descripción del evento;

7. Tipo de Evento:

a. Servicios tecnológicos;

b. Operación de los procesos;

c. Uso de inmuebles;

8. Servidor Público al que se turna la notificación.

Durante el registro de los eventos, sólo se cubrirá la Información requerida en los numerales 1 a 6.

B.5. Los Enlaces de Seguridad de la Información de las Unidades Administrativas, los Enlaces de Seguridad Informática de las Direcciones Regionales y las Subdirecciones de Informática o equivalentes en las Coordinaciones Estatales, deberán registrar en la

plataforma de Mesa de Ayuda las notificaciones de eventos de Seguridad de la Información que reciban.

C. Evaluación y toma de decisiones en torno a Eventos de Seguridad de la Información.

C.1. Corresponde a los servidores públicos del Instituto a cargo de la Mesa de Ayuda clasificar los eventos de Seguridad de la Información registrados conforme a la causa que lo originó:

1. **Servicios Informáticos:** Infección de virus, troyano, ransomware u otro tipo de código malicioso; Hackeo de Sitios o páginas web del Instituto; suplantación de identidad; acceso no autorizado a Aplicaciones Informáticas, Bases de Datos y servidores departamentales, correo electrónico sospechoso, robo o extracción de Equipamiento sin autorización;
2. **Operación en los procesos:** Borrado de Información intencional o por descuido, secuestro de Información, pérdida de Información digital o impresa, difusión no autorizada de Información, falta de acceso a la Información, pérdida de equipos de cómputo y Medios de Almacenamiento, Uso Inadecuado de información, Alteración de la Información, y
3. **Uso de inmuebles:** Personal no autorizado ingresa a zonas restringidas, visitantes, Personal Externo transita sin vigilancia, bloqueo de acceso a oficinas o inmuebles institucionales.

C.2. De acuerdo con el tipo de evento, la Dirección General Adjunta de Informática, a través de los servidores públicos del Instituto que están a cargo de la Mesa de Ayuda, asignará un nivel de prioridad conforme a los criterios que para tal efecto establezca el Comité, adicionalmente procederá a realizar las siguientes acciones:

Causa que originó el evento	Turnar	Informar
Servicios informáticos	Responsable del servicio informático correspondiente.	Titular de la Dirección General Adjunta de Informática.
Operación en los procesos	Enlace de Seguridad de la Información de la Unidad Administrativa central correspondiente.	Comité por conducto de su Presidente.

Causa que originó el evento	Turnar	Informar
	Enlaces informáticos y Subdirectores de Informática en los ámbitos regional y estatal, respectivamente.	
Uso de inmuebles	Responsable del Inmueble afectado. Enlace de Seguridad de la Información de la Dirección General de Administración.	Titular de la Dirección General Adjunta de Recursos Materiales Y servicios Generales Enlace de Seguridad de las Unidades Administrativas que cuenten con esta figura en el inmueble. Enlaces informáticos y subdirectores de informática en los ámbitos regional y estatal respectivamente.

C.3. Conforme a lo establecido en el punto C.2. del Protocolo, el servidor público al que se turne el evento de Seguridad de la Información deberá realizar las siguientes actividades:

1. Verificar la Información recabada en el reporte, es decir, que la situación efectivamente se esté presentando, y
2. Conforme al impacto en la Información, las personas y los procesos Institucionales, determinar si el evento requiere ser considerado como un Incidente de Seguridad de la Información.

C.4. Las disposiciones establecidas en el punto C.2. del Protocolo, no descartan el involucramiento y notificación a otros servidores públicos, Unidades Administrativas y entidades externas al Instituto que resulten necesarias en cumplimiento al marco normativo vigente relacionado con el tipo de afectación de que se trate.

D. Respuesta a Incidentes de Seguridad de la Información.

D.1. El Servidor Público al que se le haya turnado el Incidente, conforme a lo establecido en el punto C.2. del Protocolo, deberá coordinar las acciones necesarias para responder al Incidente considerando lo siguiente:

1. Analizará las causas del Incidente de Seguridad de la Información;

2. Identificará los impactos en los diferentes ámbitos, según la naturaleza del Incidente de Seguridad de la Información (Personas, Información, Económicos, Operación, Prestigio Institucional, entre otras);

3. Identificará, reunirá y resguardará pruebas del Incidente;

4. Según la naturaleza del Incidente, así como de los impactos ocasionados, reportar a las instancias correspondientes en cumplimiento a la normatividad aplicable a la Información y al proceso de que se trate;

5. Implementará las acciones que correspondan según la documentación existente para casos de contingencia, recuperación de desastres u otro tipo de documentos similares que determinen las acciones por realizar ante el Incidente de Seguridad de la Información en cuestión;

6. En el caso de que no exista la documentación a la que se hace referencia en el numeral anterior, se deberá de construir en el menor tiempo posible un procedimiento para:

a. Detener la progresión del daño causado por el Incidente de Seguridad de la Información;

b. Minimizar el impacto causado a las personas, la Información, la operación y el Prestigio Institucional, y

c. Para el inciso anterior, se deberá considerar la participación del personal del Instituto y áreas expertas en la temática dentro de la que se dio el Incidente de Seguridad de la Información, así como de Personal Externo y Prestadores de Servicios del Instituto.

D.2. Una vez que la respuesta al Incidente ha sido implementada, el servidor público al que se haya turnado el Incidente de Seguridad de la Información se deberá informar al Presidente del Comité, así como a las áreas afectadas o relacionadas con el Incidente.

D.3. El servidor público al que se le haya turnado el Incidente, conforme a lo establecido en el punto C.2. del Protocolo, deberá complementar la ficha de registro disponible en la Mesa de Ayuda Institucional, proporcionando la siguiente información:

1. Diagnóstico, es decir causas, vulnerabilidades y Amenazas que ocasionaron el Incidente;

2. Impactos, en las personas, la Información, la Operación, Económico, Prestigio Institucional;
3. Respuesta al Incidente de Seguridad de la Información, es decir, conjunto de acciones implementadas para contrarrestar los daños;
4. Personal involucrado en la respuesta;
5. Efectos colaterales, y
6. Evidencias.

E. Aprendizaje de los Incidentes de Seguridad de la Información.

E.1. El servidor público al que se le haya turnado el Incidente de Seguridad de la Información, conforme a lo establecido en el punto C.2. del Protocolo, deberá conformar un Grupo de Trabajo con el objetivo de analizar lo sucedido en el Incidente de Seguridad de la Información. Para la Integración del Grupo de Trabajo, se deberán tomar en cuenta las siguientes consideraciones:

1. El Grupo de Trabajo se deberá conformar a más tardar transcurridos quince días naturales posteriores a que haya finalizado la respuesta al Incidente de Seguridad de la Información, y
2. El Grupo de Trabajo se conformará por el personal que estuvo involucrado en la respuesta al Incidente de Seguridad de la Información, así como representantes del proceso, servicio, inmueble o Unidad o Área Administrativa afectados.

E.2. El Grupo de Trabajo deberá entregar al Comité en un plazo no mayor a treinta días naturales contados a partir de su conformación, un informe del resultado del análisis realizado sobre el Incidente de Seguridad de la Información en el que se considere al menos lo siguiente:

1. Posibilidad estimada de que el Incidente de Seguridad de la Información se vuelva a presentar;
2. Vulnerabilidades y Amenazas relacionadas con el Incidente de Seguridad de la Información, y
3. Propuesta de acciones para reducir la posibilidad de que el Incidente de Seguridad de la Información vuelva a ocurrir.

E.3. La Unidad o Área Administrativa que tenga bajo su responsabilidad la Información, el proceso, proyecto, servicio o inmueble afectado, deberá considerar el Informe señalado en el punto E.2. del Protocolo a efecto de tomar las medidas posibles para que el Incidente de Seguridad de la Información no ocurra nuevamente, considerando lo siguiente:

1. Realizar una Matriz de Administración de Riesgos o revisar la existente en cumplimiento a lo dispuesto por la Metodología para la Administración de Riesgos emitida por la Contraloría Interna;

2. Desarrollar un Plan de Contingencia y Plan de Recuperación de Desastres o actualizar los existentes, y

3. Realizar pruebas y simulacros con el objeto de comprobar la efectividad de las medidas descritas en los incisos de este punto del Protocolo.

F. INTERPRETACIÓN.

Corresponde al titular de la Dirección General de Integración, Análisis e Investigación la interpretación de este Protocolo para efectos administrativos.

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

TRANSITORIOS

PRIMERO.- El Presente Protocolo entrará en vigor al día siguiente de su publicación en la Normateca Interna del Instituto.

SEGUNDO.- El Módulo de Registro de Notificación de Eventos al que hace referencia el punto B.4. del Protocolo, así como los criterios para asignar prioridad señalados en el punto C.2., deberán aprobarse a más tardar transcurridos 90 días hábiles a partir de la entrada en vigor del Protocolo.

TERCERO.- Con el fin de fomentar el registro de los incidentes en materia de Seguridad de la Información, las Unidades y Áreas Administrativas deberán documentar los incidentes de Seguridad de la Información acontecidos en su ámbito de competencia antes de la entrada en vigor del presente Protocolo, conforme a los criterios que para ello defina el Comité, los cuales

deberán aprobarse a más tardar transcurridos 90 días hábiles a partir de la entrada en vigor del Protocolo.

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-03/ORD-2/2015.

Última hoja del Protocolo Institucional de Respuesta a Incidentes de Seguridad de la Información, el cual se hace constar de 12 fojas útiles y fue publicado en la Normateca Interna del Instituto con fecha 07 de agosto de 2015.