INSTITUTO NACIONAL
DE ESTADÍSTICA Y GEOGRAFÍA

CRITERIOS PARA LA DOCUMENTACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

COMITÉ DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN.

DICIEMBRE 2015.
Aguascalientes, Aguascalientes.

ÍNDICE

INTRODUCCIÓN 3

1. Criterios Generales. 4

2. Criterios Específicos. 5

TRANSITORIOS 7

INTRODUCCIÓN

El Protocolo Institucional de Respuesta a Incidentes de Seguridad de la Información publicado el 7 de agosto de 2015 establece las líneas de acción a partir de las cuales deberán atenderse los Incidentes de Seguridad de la Información que ocurran en el Instituto. Uno de los aspectos considerados en el Protocolo es el aprendizaje generado a partir del análisis y atención de los incidentes, en tal sentido el presente documento tiene por objetivo definir los criterios que deben seguir las Unidades y Áreas Administrativas para documentar los incidentes de seguridad de la información ocurridos previo a la entrada en vigor del Protocolo, contribuyendo así al aprendizaje en la materia y al fortalecimiento de la seguridad de la información.

Considerando lo anterior y conforme a lo establecido en el *Manual de Integración y Funcionamiento del Comité del Sistema de Seguridad de la Información*, apartado VI, numeral 6.3.1, inciso a), así como en cumplimiento a lo dispuesto por el artículo 41 y Segundo Transitorio de los *Lineamientos para el Fortalecimiento de la Seguridad de la Información en los Procesos y Servicios Institucionales,* los miembros del Comité del Sistema de Seguridad de la Información han tenido a bien emitir los siguientes:

CRITERIOS PARA LA DOCUMENTACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

1. Criterios Generales.

1.1. Objetivo.-

Establecer los criterios que deben seguir las Unidades y Áreas Administrativas para documentar los Incidentes de Seguridad de la información que hayan ocurrido previo a la entrada en vigor del *Protocolo Institucional de Respuesta a Incidentes de Seguridad de la Información*, con lo que se fomenta el registro de éstos y favorece el aprendizaje en la materia.

1.2. Ámbito de Aplicación.-

Los presentes Criterios son de observancia general para las Unidades y Áreas Administrativas del Instituto, así como a los servidores públicos adscritos a las mismas, con la finalidad de fomentar el registro de los Incidentes de Seguridad de la Información.

1.3. Glosario.-

Resultan aplicables los conceptos contenidos en el punto A.3. del Protocolo Institucional de Respuesta a Incidentes de Seguridad de la Información;, así mismo, para efectos de los presentes Lineamientos se entenderá por:

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

II. **Comité:** Comité del Sistema de Seguridad de la Información;

III. **Criterios:** Criterios para la documentación de incidentes de Seguridad de la Información;

IV. **Evidencias:** Conjunto de pruebas que dejan vestigio de un Incidente de Seguridad de la Información, sus causas e impactos;

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

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

VII. **Prestigio Institucional:** Credibilidad y confianza que la sociedad ha depositado en el Instituto, y

VIII. **Protocolo:** Protocolo Institucional de Respuesta a Incidentes de Seguridad de la Información del Instituto Nacional de Estadística y Geografía.

2. Criterios Específicos.

2.1. De los Informes sobre incidentes de seguridad de la información.-

Las Unidades y Áreas Administrativas, a través de sus Enlaces de Seguridad de la Información realizarán un informe en el que se documenten los incidentes que ocasionaron la pérdida de confidencialidad, integridad o disponibilidad de la información independientemente de su origen, por servicios informáticos, operación en los procesos o uso de inmuebles.

a) **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;
b) **Operación en los procesos:** Borrado de Información intencional o por descuido, secuestro o robo 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
c) **Uso de inmuebles:** Personal no autorizado ingresa a zonas restringidas, visitantes, Personal Externo transita sin vigilancia, bloqueo de acceso a oficinas o inmuebles institucionales.

El informe se dirigirá, mediante nota, al Presidente del Comité del Sistema de Seguridad de la Información para su análisis.

2.2. Del período de aplicación.-

Los incidentes de seguridad de la información a documentar serán los acontecidos en el Instituto en el período comprendido entre el 01/01/2014 y el 06/08/2015. Sin embargo, se podrán documentar todos los incidentes ocurridos en fechas previas al período señalado y que a juicio de los Enlaces de Seguridad de la Información resulten relevantes por el impacto ocasionado en el Instituto y el aprendizaje que se puede obtener de su análisis.

2.3. De los datos a documentar.-

El informe referido en el punto 2.1. debe contener los siguientes datos:

a) Fecha en que ocurrió el incidente;
b) Sitio donde tuvo lugar el incidente (Entidad Federativa, Municipio, edificio y oficina);
c) Unidad o Área Administrativa relacionada con el incidente;
d) Procesos, proyectos, servicios y productos o Información afectados;
e) Descripción del incidente;
f) Origen del incidente:
    a. Servicios tecnológicos;
    b. Operación de los procesos, y
    c. Uso de inmuebles.
g) Causas del incidente:
    a. Amenazas, y
    b. Vulnerabilidades.
h) Impactos ocasionados por el incidente:
    a. Personas;
    b. Información;
    c. Económicos;
    d. Operación;
    e. Prestigio Institucional, y
    f. Otros.
i) Respuesta al incidente;
    a. Medidas preventivas para evitar que se vuelva a presentar el incidente, y
    b. Medidas correctivas para disminuir el impacto del incidente en caso de que se vuelva a presentar.
j) Servidores públicos involucrados en la respuesta;

k) Posibilidad estimada de que el incidente se vuelva a presentar, y

l) Evidencias del incidente, de existir.

2.4. Interpretación.-

Corresponde al Titular de la Dirección General de Integración, Análisis e Investigación la interpretación de los Criterios para efectos administrativos.

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

TRANSITORIOS

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

SEGUNDO.- Las Unidades Administrativas del instituto contarán con noventa días hábiles a partir de la entrada en vigor de este instrumento para documentar e informar al Presidente del Comité sobre los incidentes de seguridad de la información ocurridos en su ámbito de competencia referidos al período de aplicación de los presentes Criterios.

El presente documento fue aprobado en la Sesión Ordinaria 03 2015 del Comité del Sistema de Seguridad de la Información, celebrada el día 15 de diciembre de 2015, mediante Acuerdo CSSI- 006/ORD-3/2015.

Última hoja de los Criterios de documentación de Incidentes de Seguridad de la Información, el cual se hace constar de 7 fojas útiles y fue publicado en la Normateca Interna del Instituto con fecha 20 de enero de 2016.