INSTITUTO NACIONAL
DE ESTADÍSTICA Y GEOGRAFÍA

CRITERIOS PARA ASIGNAR PRIORIDAD A LOS EVENTOS DE SEGURIDAD DE LA INFORMACIÓN.

COMITÉ DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN.

DICIEMBRE 2015.
Aguascalientes, Aguascalientes.

ÍNDICE

INTRODUCCIÓN

La identificación, documentación solución y seguimiento de Incidentes de Seguridad de la Información juega un papel importante en toda organización que aspire a proteger su información que se requiere de la presencia de varios factores como: personal comprometido y en estado de alerta; canales de notificación, y protocolos de respuesta, documentación y aprendizaje. Adicionalmente, es necesario definir los criterios que permitan asignar prioridades a cada una de las notificaciones de eventos de 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), el artículo 4 de los *Lineamientos para el Fortalecimiento de la Seguridad de la Información en los Procesos y Servicios Institucionales*, así como en cumplimiento al dispuesto por el punto C.2. del *Protocolo Institucional de Respuesta a Incidentes de Seguridad de la Información*, los miembros del Comité del Sistema de Seguridad de la Información han tenido a bien emitir los siguientes:

CRITERIOS PARA ASIGNAR PRIORIDAD A LOS EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

1. Criterios Generales.

1.1. Objetivo.-

Establecer los criterios y procedimientos necesarios para asignar un nivel de prioridad a los eventos de Seguridad de la Información que se registren en el Módulo de Mesa de Ayuda.

1.2. Ámbito de Aplicación.-

Los presentes Criterios son de observancia general para las servidoras y los servidores públicos que formen parte del esquema de Mesa de Ayuda tanto en Oficinas Centrales como en las Direcciones Regionales y Coordinaciones Estatales.

1.3. Glosario.-

Resultan aplicables los conceptos contenidos en el apartado A.3 del Protocolo Institucional de Respuesta a Incidentes de Seguridad de la Información.

2. Criterios Específicos.

2.1. Consideraciones generales.-

a) Todas las notificaciones de Eventos de Seguridad de la Información sin excepción alguna deberán registrarse en el Módulo correspondiente en la Módulo de Mesa de Ayuda;

b) El cálculo para asignar prioridad a los eventos de Seguridad de la Información se realizará tomando en cuenta el estado o nivel de progresión del evento, así como el impacto ocasionado;

c) Para asignar la prioridad a los eventos de Seguridad de la Información el personal de Mesa de Ayuda deberá basarse en la información que proporcione quien hace el reporte. Si la información no es lo suficientemente clara para asignar un nivel determinado, se debe procurar asociarlo con el nivel cuya descripción sea más cercano a lo que está ocurriendo, y

d) El Nivel de Prioridad se calculará de manera automática conforme a lo establecido en el apartado 2.2 de los presentes Criterios y formará parte del registro del evento en el Módulo correspondiente.

2.2. Cálculo del Nivel de Prioridad.-

El cálculo del nivel de prioridad del evento se realiza mediante la asignación de valores numéricos a cada dimensión de las variables, estado e impacto.

En las siguientes tablas se relacionan los valores correspondientes con cada dimensión de las variables mencionadas.

Tabla 1. Valores determinados conforme al estado del evento.

Estatus	Valor
Está en progreso.	2
Está por ocurrir.	1.5
Ya ocurrió.	1

Tabla 2. Valores a asignar conforme al Impacto ocasionado por el evento.

Impacto	Valor
Ocasiona un incumplimiento legal o normativo.	3
Ocasiona pérdida de confianza por parte de los informantes o público en general.	3
Interrupción total del proceso.	2
Ocasiona daño en la infraestructura material del Instituto.	2
Ninguna de las anteriores.	1

Para asignar el nivel de prioridad, primero se calcula un Índice de prioridad (*IP)* aplicando la siguiente fórmula que consiste en multiplicar los valores del Estatus del evento con el Impacto del evento:

IP = Ee . Ie

Dónde:

Ee: Estado del evento.

Ie: Impacto del evento.

Según el ***IP***, se determina el nivel de prioridad conforme a los rangos que se relacionan en la tabla siguiente.

Tabla 3. Rango de valores por nivel de prioridad.

Prioridad	Rango
A	4 – 6
B	2 – 3
C	1 – 1.5

Ejemplo:

Notificación: Hemos identificado que se han robado documentación de una bodega del instituto, al parecer se trataba de información contable.

Asociación de variables:

Estatus del Evento: Ya ocurrió (1).

Impacto del Evento: Ocasiona un incumplimiento legal o normativo (3).

Cálculo del IP: Ee (1) . Ie (3) = 3.

Prioridad del Evento: B.

2.3. Criterios para determinar la variable Estatus:

Se refiere al nivel de avance del evento, lo anterior permitirá conocer el margen de actuación y el tipo de acciones que se pueden realizar:

1. **Está en progreso:** Ya hubo una afectación, la amenaza se materializó, el hecho se está produciendo en el momento y el daño a la información está aumentando a medida que pasa el tiempo.

   Ejemplos:

   a) *Hay un grupo de protesta que está plantado en el exterior de las oficinas del Instituto, no permite la entrada ni salida de personal y han anunciado que estarán tres días más. Lo anterior ha ocasionado que los servidores públicos no puedan acceder a la información almacenada en sus equipos de cómputo y material impreso.*

   b) *El Sitio del Instituto en Internet está siendo bombardeado con muchas peticiones, puede ser un DoS (de las siglas en inglés Denial of Service, Ataque de denegación de servicio).*

2. **Está por ocurrir:** El riesgo aún no se ha materializado, es decir, no se ha causado un daño a la información, sin embargo todo apunta a que en lo inmediato podrá suceder con un muy alto índice de probabilidad.

   Ejemplos:

   a) *Se ha anunciado que un grupo de protesta realizará un plantón en el exterior de las oficinas del Instituto, se espera que lleguen hoy al medio día. Lo anterior podría ocasionar que los servidores públicos no puedan acceder a la información almacenada en sus equipos de cómputo y material impreso.*

   b) *Un fabricante de Software para desarrollo de aplicaciones informáticas emitió un comunicado en el que da a conocer una vulnerabilidad que puede ser explotada, cabe señalar que es el software que se utilizó en las aplicaciones involucradas en el levantamiento de información.*

   c) *Repentinamente una carpeta compartida a través de FTP ha dejado de solicitar cuenta de usuario y se puede acceder de manera anónima (sin proporcionar nombre de usuario y contraseña), cabe señalar que es el repositorio donde se deposita información que sólo puede conocer un número limitado de personas.*

3. **Ya ocurrió:** El riesgo se materializó, causó daños y el agente dañino se retiró o dejó de existir.

   Ejemplos:

a) *En la mañana al iniciar labores, se encontró que un archivero que guarda información importante estaba abierto con evidencias de que alguien forzó la cerradura, al revisar el interior se descubrió que faltaban dos expedientes completos.*

b) *Fue vulnerada la seguridad de una página del sitio del Instituto en* Internet *a través de la cual se publicaba información, en su lugar aparece un mensaje de protesta.*

c) *Se perdieron carpetas electrónicas con información relativa al levantamiento de información de la Encuesta.*

2.4. Criterios para determinar la variable Impacto.-

Se refiere a los daños ocasionados o que se podrían ocasionar. El impacto se puede caracterizar de la siguiente manera:

1. **Pone en peligro al personal (interno y externo):** La información ha resultado afectada *(acceso o divulgación sin autorización, pérdida total o parcial, alteración, inaccesibilidad)* y adicionalmente la salud e integridad física de las personas se encuentra en peligro.

   Ejemplos:

   a) *Incendio en una bodega que almacena expedientes, al parecer también hay oficinas ocupadas por personal al interior o cercanas a la misma.*

   b) *Robo de equipo de dispositivos móviles a personal que se encontraba en el operativo de levantamiento de información en campo, al parecer fue robo con violencia.*

2. **Ocasiona un incumplimiento legal o normativo:** La información ha resultado afectada *(acceso o divulgación sin autorización, pérdida total o parcial, alteración, inaccesibilidad).* Entre otras consecuencias, se ha incumplido con una responsabilidad legal, o bien, alguna obligación adquirida a partir de un acuerdo de voluntades.

   Ejemplos:

   a) *Se publicó la base de datos que contenía los datos de los informantes de forma nominativa en Internet, varios usuarios del sistema se dieron cuenta.*

b) Se ha dado a conocer información en posesión del Instituto, la cual se obtuvo a partir de un convenio con otra institución y que en el contrato se estableció que sólo ésta última podría hacer uso de ella.

3. **Ocasiona pérdida de confianza por parte de los informantes o público en general:** La información ha resultado afectada *(acceso o divulgación sin autorización, pérdida total o parcial, alteración, inaccesibilidad).* Entre otras consecuencias, ha ocasionado o puede ocasionar que los informantes ya no quieran proporcionar información al Instituto.

   Ejemplos:

   a) Durante una encuesta, se quedaron olvidados en una oficina u hogar algunos instrumentos de recolección con información de otros informantes relacionados con el mismo proyecto.

   b) Al acceder a la aplicación de recopilación de datos por Internet, los datos de otros informantes quedaron disponibles para descargarse.

4. **Interrupción total del proceso:** La información ha resultado afectada *(acceso o divulgación sin autorización, pérdida total o parcial, alteración, inaccesibilidad).* Entre otras consecuencias, ha interrumpido la operación del proceso.

   Ejemplos:

   a) No se puede acceder a la base de datos que se está revisando y sobre la cual se están ejecutando procedimientos de validación.

5. **Ocasiona daño en la infraestructura del Instituto:** La información ha resultado afectada *(acceso o divulgación sin autorización, pérdida total o parcial, alteración, inaccesibilidad).* Entre otras consecuencias, algún componente de la infraestructura del Instituto (bienes muebles e inmuebles y servicios) ha sufrido algún daño.

   Ejemplos:

   a) Incendio en una bodega de expedientes, incendio o inundación en oficinas

6. **Ninguna de las anteriores:** Los hechos descritos durante la notificación no proporcionan suficientes elementos para asociarla a algún tipo de impacto.

2.5. 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.

TRANSITORIO

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

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-007/ORD-3/2015.

Última hoja de los Criterios para asignar prioridad a los eventos de seguridad de la información, el cual se hace constar de 10 fojas útiles y fue publicado en la Normateca Interna del Instituto con fecha 20 de enero de 2016.