INSTITUTO NACIONAL
DE ESTADÍSTICA Y GEOGRAFÍA

CRITERIOS GENERALES PARA LA PROTECCIÓN Y RESGUARDO DE LA INFORMACIÓN CON BASE EN SUS CONTENIDOS.

COMITÉ DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN.

DICIEMBRE 2015.
Aguascalientes, Aguascalientes.

ÍNDICE

INTRODUCCIÓN 3

1. Criterios Generales. 4

2. Criterios Específicos. 4

TRANSITORIO 8

INTRODUCCIÓN

Los presentes criterios generales son una referencia para contribuir a la protección y resguardo de los Activos de Información conforme a sus requerimientos en materia de Confidencialidad, Integridad y Disponibilidad; representan un complemento a los Criterios para la calificación de Activos de Información con los que se obtiene una calificación global por activo que posibilita asignar prioridades para establecer medidas de seguridad de la información.

Considerando lo anterior y conforme a las atribuciones establecidas 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 4 de los *Lineamientos para el Fortalecimiento de la Seguridad de la Información en los Procesos y Servicios Institucionales*, en atención a los aspectos transversales en materia de Seguridad de la Información, los miembros del Comité del Sistema de Seguridad de la Información han tenido a bien emitir los siguientes:

CRITERIOS GENERALES PARA LA PROTECCIÓN Y RESGUARDO DE LA INFORMACIÓN CON BASE EN SUS CONTENIDOS

1. Criterios Generales.

1.1. Objetivo.-

Establecer los criterios que deben seguir las Unidades y Áreas Administrativas para implementar esquemas que contribuyan a la protección y resguardo de los Activos de Información que forman parte del Listado de Activos de Información.

1.2. Ámbito de Aplicación.-

Los presentes Criterios son de observancia general para las Unidades y Áreas Administrativas del Instituto, así como por las servidoras y los servidores públicos adscritos a las mismas, como complemento a las acciones implementadas a partir de los *Criterios para la calificación de los Activos de Información*.

1.3. Glosario.-

Resultan aplicables los conceptos contenidos en el Artículo 6, de los Lineamientos para el Fortalecimiento de la Seguridad de la Información en los procesos y servicios institucionales, así mismo para efectos de los presentes Criterios se entenderá por:

I. **Código hash:** Cadena de caracteres que se crea a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) y que solo puede volverse a crear con esos mismos datos, se utiliza frecuentemente como un elemento para verificar la Integridad de la Información.

2. Criterios Específicos.

2.1. Consideraciones.-

a) Los presentes Criterios son aplicables a los Activos de Información cuya Calificación Global sea igual o mayor a 48, conforme a la calificación obtenida en el Anexo I de los Criterios para la calificación de Activos de Información;

b) Para aquellos Activos de Información cuya Calificación Global sea igual a 64, deberá realizarse un ejercicio de Administración de Riesgos considerando la Normatividad administrativa Institucional en la materia;

c) Los presentes Criterios, no excluyen la aplicación de otras medidas que apliquen a los Activos de Información en términos de la legislación y normatividad aplicable. De la misma manera, tampoco excluyen la observancia de controles adicionales propuestos por los responsables de los Activos de Información;

d) Los presentes Criterios deberán aplicarse siempre, excepto cuando el Vocal del Comité del Sistema de Seguridad de la Información representante de la Unidad Administrativa respectiva considere que su aplicación compromete la continuidad de los procesos, en cuyo caso debe documentar esta decisión;

e) Corresponde a los responsables de los Activos de Información coordinar la aplicación de los presentes Criterios en su respectivo ámbito de competencia.

2.2. Criterios para proteger y resguardar la información con base en los requerimientos de Confidencialidad.-

a) Para los Activos de Información con requerimientos en **Confidencialidad nivel ALTO**:

I. Implementar controles informáticos y físicos que contribuyan a reducir la posibilidad de que se presenten accesos no autorizados a los Activos de Información;

II. Implementar procedimientos claros y viables para solicitar, autorizar, modificar o revocar los permisos de acceso a los Activos de Información;

III. Por cada Activo de Información, Identificar los requerimientos y procedimientos de seguridad a los que están sujetos conforme a la legislación y normatividad aplicable;

IV. Revisar y actualizar por lo menos una vez al año la lista del personal autorizado para acceder a los Activos de Información de manera que se revoquen los permisos respecto de los cuales no subsistan las causas que motivaron su otorgamiento;

V. Llevar a cabo por lo menos una vez al año simulacros de ingreso no autorizado, es decir, representar un ataque simulado con la intención de encontrar debilidades en materia de seguridad de la Información, y

VI. Conforme al ciclo de vida de cada Activo de Información, llevar a cabo los procedimientos de eliminación o conservación según corresponda de acuerdo a la legislación y normatividad aplicables.

b) Para los Activos de Información con requerimientos en **Confidencialidad nivel MEDIO:**

I. Implementar procedimientos claros y viables para solicitar, autorizar, modificar o revocar permisos de acceso a los Activos de Información.

2.3. Criterios para proteger y resguardar la información con base en los requerimientos de Integridad.-

a) Para los Activos de Información con requerimientos de **Integridad nivel ALTO**:

I. Implementar controles informáticos y físicos que contribuyan a reducir la posibilidad de que se presenten accesos no autorizados borren o modifiquen los Activos de Información;

II. Para el caso de Activos de Información con valor histórico y con poca dinámica de actualización o cuya etapa de modificación haya concluido y que deban conservarse cumplimiento a la legislación y normatividad aplicables, se considerará la aplicación de procedimientos de verificación que contengan mecanismos para comprobar la integridad, como *código hash* y otras alternativas;

III. Implementar procedimientos claros y viables para solicitar, autorizar, modificar o revocar los permisos de acceso a los Activos de Información;

IV. Revisar y actualizar periódicamente y actualizar siempre que resulte necesario, la lista del personal autorizado para acceder a los Activos de Información de manera que se puedan revocar los permisos a aquellos Servidores Públicos que por cambio de funciones o término de encargo o comisión ya no deban acceder;

V. Llevar a cabo por lo menos una vez al año simulacros y simular un ataque con la intención de encontrar las debilidades en materia de seguridad de la información;

VI. Establecer procedimientos de control de versiones y documentación de cambios;

VII. En cuanto sea posible, habilitar bitácoras automáticas que registren los accesos y tipo de operación realizada a los Activos de Información, y

b) Para los Activos de Información con requerimientos en **Integridad nivel MEDIO**:

I. Implementar controles informáticos y físicos que contribuyan a reducir la posibilidad de que se presenten accesos no autorizados borren o modifiquen los Activos de Información;

II. Establecer procedimientos de control de versiones y documentación de cambios.

III. Habilitar bitácoras automáticas que registren los accesos y tipo de operación realizada a los Activos de Información, y

2.4. Criterios para proteger y resguardar la información con base en los requerimientos de Disponibilidad.-

a) Para los Activos de Información con requerimientos en **Disponibilidad nivel ALTO**:

I. Implementar mecanismos que proporcionen redundancia para el acceso a los Activos de Información;

II. Llevar a cabo por lo menos una vez al año simulacros para identificar posibles causas e impactos que ocasionaría la indisponibilidad de los Activos de Información con el propósito de establecer medidas de contingencia, y

III. Establecer planes de respaldos en cuando a los Activos de Información y de los medios necesarios para acceder a ellos.

b) Para los Activos de Información con requerimientos en **Disponibilidad nivel MEDIO**:

I. Establecer planes de respaldos en cuando a los Activos de Información y de los medios necesarios para acceder a ellos.

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-003/ORD-3/2015.

Última hoja de los Criterios generales para la protección y resguardo de la información con base en sus contenidos, el cual se hace constar de 8 fojas útiles y fue publicado en la Normateca Interna del Instituto con fecha 20 de enero de 2016.