PRESIDENCIA DE LA REPÚBLICA

LINEAMIENTO PARA GESTION DE INCIDENTES Y VULNERABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

Bogotá D.C. Diciembre de 2017

TABLA DE CONTENIDO

1. OBJETIVO ---------- 3
2. ALCANCE ---------- 3
3. TÉRMINOS Y DEFINICIONES ---------- 3
4. ÁMBITO DE APLICACIÓN Y DISPOSICIONES GENERALES ---------- 3
   4.1.1 Lineamientos para la gestión de incidentes de seguridad de la información ---------- 3
   4.1.2 Lineamiento para la gestión de vulnerabilidades ---------- 4
5. MARCO LEGAL ---------- 4
6. DOCUMENTOS ASOCIADOS ---------- 4
7. RESPONSABLE DEL DOCUMENTO ---------- 5

1. OBJETIVO

Asegurar que los eventos, incidentes y vulnerabilidades de seguridad que se presenten con los activos de información, sean comunicados y atendidos oportunamente empleando las acciones o actividades, con el fin de aplicar de manera oportuna las acciones correctivas

2. ALCANCE

Estos lineamientos deben ser aplicados por todos los funcionarios, contratistas, pasantes, personal en comisión, del Departamento Administrativo de la Presidencia de la República.

3. TÉRMINOS Y DEFINICIONES

Almacenamiento de red personal (Nube): Incluye el acceso a páginas Web que permiten a los usuarios subir carpetas y archivos a un servidor de red en línea para realizar copias de seguridad, compartir, editar o recuperar archivos o carpetas desde cualquier navegador Web. (Este almacenamiento desde los servicios de TI debe tener la configuración de herramientas de prevención de pérdidas de información del DAPRE, realizadas por el Área de Tecnologías y Sistemas de Información.)

Red: es el sistema de conexión de un grupo de computadoras o equipos activos que permiten el envío de información entre sí.

4. ÁMBITO DE APLICACIÓN Y DISPOSICIONES GENERALES

Los lineamientos para la gestión de incidentes y vulnerabilidades de seguridad de la información se desarrollarán bajo la coordinación del Comité de Seguridad de la Información de la Entidad, el CSIRT (Computer Security Incident Response) - Equipo de Respuesta ante Incidentes de Seguridad Informática de la Casa Militar y el Área de Tecnologías y Sistemas de la Información.

4.1.1 Lineamientos para la gestión de incidentes de seguridad de la información

El DAPRE establecerá responsables y procedimientos de gestión para el tratamiento de incidentes de seguridad de la información asegurando una respuesta rápida, eficaz y eficiente, quienes investigarán y solucionarán los incidentes presentados, implementando las acciones necesarias para evitar su repetición, así mismo debe escalar los incidentes de acuerdo con la criticidad del mismo.

El único canal acreditado para reportar incidentes de seguridad ante las autoridades y el pronunciamiento oficial ante entidades externas de la Presidencia de la República es el Director del Departamento o el funcionario que sea delegado.
El DAPRE designa al Área de Tecnologías y Sistemas de Información para responder a los eventos o incidentes de seguridad informática, de acuerdo a las sugerencias, recomendaciones y/o acompañamiento del CSIRT

(Computer Security Incident Response) - Equipo de Respuesta ante Incidentes de Seguridad Informática de la Casa Militar; debe generarse el procedimiento de respuesta.

Casa Militar será el encargado de coordinar y adelantar las gestiones pertinentes para la atención de los eventos o incidentes de seguridad de la información.

Se debe establecer la implementación de lecciones aprendidas al término del análisis y solución de incidentes de seguridad de la información, estos deben ser socializados a los interesados conservando la confidencialidad de estas, así mismo, estas deben ser utilizadas como herramienta para la toma de decisiones y revisiones de la política de seguridad.

El CSIRT (Computer Security Incident Response) Equipo de respuesta a incidentes de seguridad informática debe establecer el procedimiento para la recolección de evidencia digital, siguiendo los lineamientos jurídicos vigentes en Colombia y estándares internacionales.

4.1.2 Lineamiento para la gestión de vulnerabilidades

El Área de Tecnologías y Sistemas de Información en coordinación con el CSIRT (Computer Security Incident Response Team) Equipo de respuesta a incidentes de seguridad informática de la Casa Militar, realizará pruebas técnicas de vulnerabilidad a intervalos planificados en los sistemas de información y comunicaciones del DAPRE.

El Área de Tecnologías y Sistemas de Información implementará un programa de gestión de vulnerabilidades técnicas que incluya el plan de tratamiento de vulnerabilidades, el cual deberá ser aprobado por el Comité de Seguridad de la Información.

5. MARCO LEGAL

- ✓ Ley 1581 de 2012
- ✓ Decreto 1377 de 2013
- ✓ Ley 1273 de 2009
- ✓ Decreto 415 de 2016
- ✓ Decreto 2573 de 2015
- ✓ Ley 1712 de 2014
- ✓ Resolución 3564 de 2015
- ✓ Ley 1266 de 2008
- ✓ Decreto 2364 de 2012

6. DOCUMENTOS ASOCIADOS

- ✓ M-TI-01 Manual de Seguridad de la Información
- ✓ P-SA-03 Atención de incidentes de seguridad
- ✓ F-SA-18 Atención de incidente
- ✓ P-TI-17 Administración de Incidentes

7. RESPONSABLE DEL DOCUMENTO

Jefe Área de Tecnologías y Sistemas de Información