1. OBJETIVO

Establecer la metodología para detectar, identificar, analizar y gestionar las vulnerabilidades de los sistemas de información y de los activos de infraestructura tecnológica que soportan la operación informática de la entidad, que permita al INSTITUTO PARA LA ECONOMIA SOCIAL - IPES, prevenir, y de ser necesario, dar respuesta oportuna a incidentes de seguridad de la información.

2. ALCANCE

Aplica a funcionarios, contratistas, proveedores y terceros con acceso autorizado a los recursos de información y activos de infraestructura tecnológica del INSTITUTO PARA LA ECONOMIA SOCIAL, así como a todos los activos de información y los medios que los contengan.

4. CONDICIONES GENERALES

El crecimiento de los sistemas y servicios informáticos que apoyan el cumplimiento de los objetivos y la misión de la entidad, así como el uso de nuevas tecnologías de información y comunicaciones de apoyo en el desarrollo de las actividades institucionales, conllevan a un incremento significativo de amenazas informáticas que, pueden comprometer los activos de infraestructura tecnológica así como la información institucional critica para la toma de decisiones.

Considerando la criticidad de la información y la protección de los activos que la soportan, la respuesta a incidentes de seguridad se consolida como una herramienta estratégica que permite a la entidad, no solo estar en la capacidad de dar respuesta oportuna a incidentes de seguridad, sino también detectar, evaluar y gestionar las vulnerabilidades de la plataforma tecnológica que soporta la operación informática, de los sistemas de información misional, de gestión administrativa y de apoyo, y principalmente de los medios que alojan los activos de información del Instituto para la Economía Social - IPES.

Algunos de los beneficios de contar con una capacidad adecuada para responder a los incidentes de seguridad de la información incluyen:

- El procedimiento de gestión de incidentes es sistemático y de esa forma se pueden tomar los pasos apropiados y realizar seguimiento a los mismos.
- Contar con personal de gestión, con competencias apropiadas para dar respuesta oportuna y eficiente a los incidentes de seguridad, permite a la entidad minimizar riesgos asociados a pérdida o daño de información e indisponibilidad de servicios informáticos.
- La información recolectada durante el manejo de un incidente, se puede usar para estar mejor preparado frente a la posibilidad de materialización de incidentes futuros. La

documentación relacionada permite contar con mejores controles sobre los sistemas y servicios informáticos y sobre la información de la entidad.

- Se puede contar con una mejor preparación legal frente los problemas que se puedan generar relacionados con el incidente.

5. RESPONSABILIDADES

Es responsabilidad del Comité de Sistemas y Seguridad de la Información del INSTITUTO PARA LA ECONOMIA SOCIAL, garantizar la aplicación del procedimiento y el instructivo de manejo de incidentes, actualizarlo y evaluar las acciones de mejora que se identifiquen del tratamiento de los incidentes de seguridad que sean detectados.

3. DEFINICIONES

a. **Acción preventiva:** Conjunto de acciones tomadas para eliminar la(s) causa(s) de una no conformidad potencial u otra situación potencialmente indeseable. NOTA 1: Puede haber más de una causa para una no conformidad potencial. NOTA 2: La acción preventiva se toma para prevenir que algo suceda, mientras que la acción correctiva se toma para prevenir que vuelva a producirse.

b. **Evento:** Un evento es cualquier situación observable en el comportamiento de un equipo o servicio de tecnología. Los eventos pueden ser normales o anormales. Algunos ejemplos de eventos incluyen situaciones como: ingreso de un usuario a la red de computadores, el inicio de una copia de respaldo, la verificación de la dirección de destino de correo electrónico por parte del servidor de correo, un usuario enviando un correo electrónico, un firewall bloqueando una conexión no autorizada. Los eventos pueden tener efectos negativos para los servicios o equipos de información o tecnología, como por ejemplo: caída de servicios, saturación de canales de red, fallas en los sistemas de respaldo de información, energía o refrigeración, acceso no autorizado a sistemas o información confidencial, ejecución de código malicioso o destrucción de equipos.

c. **Incidente de seguridad:** Un incidente de seguridad de la información ("incidente") es cualquier evento que daña o representa una amenaza seria para toda o una parte de la infraestructura de información y tecnología del INSTITUTO PARA LA ECONOMIA SOCIAL (sistemas de cómputo, sistemas de información, sistemas de telefonía), como pueden ser: ausencia de servicios, inhibición para el uso de sistemas de información, incluyendo cambios no autorizados al hardware, firmware, software o datos, crímenes definidos en la ley 1273 de 2009 u otras normas que cobijen a la entidad.

d. **Incidente de seguridad computacional:** Un incidente de seguridad computacional es una violación o potencial amenaza de violación de las políticas de seguridad de la información, los procedimientos de seguridad de la información o la reglamentación que

cobija el uso de los servicios o equipos de información de tecnología. Algunos ejemplos de incidente computacional incluyen:

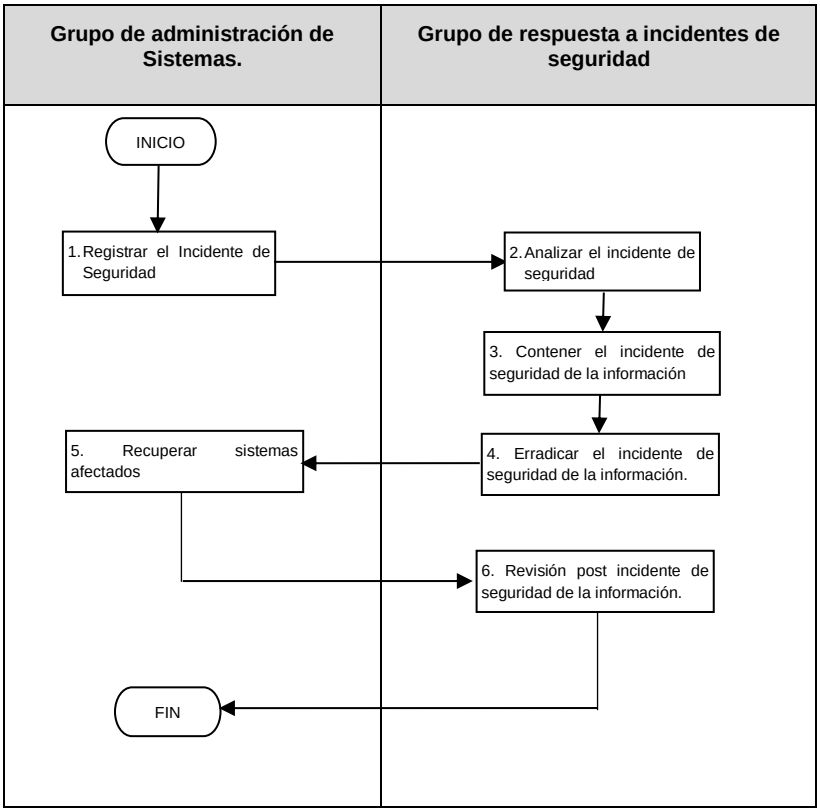
- **Denegación de servicios**: Un atacante envía un paquete de datos que bloquea o congestiona el servidor de páginas web y suspende el sitio web. Un atacante coordina a miles de estaciones de trabajo externas a la red para que envíen miles de solicitudes ICMP a la red de la entidad para que se inhabiliten los servicios de red.
- **Código malicioso**: Un gusano informático usa archivos compartidos para contaminar cientos de estaciones dentro de la entidad. La entidad recibe un reporte del vendedor de sus antivirus en donde alerta de un virus que se dispersa a gran velocidad mediante correo electrónico por Internet. El virus aprovecha una vulnerabilidad presente en los servidores de la entidad, basado en la experiencia de la entidad en otros incidentes se estima que el virus podría afectar a los equipos en un lapso de tres horas.
- **Acceso no autorizado:** Un atacante utiliza una herramienta de explotación de vulnerabilidades para tener acceso al archivo de password de usuarios. Un perpetrador obtiene acceso no autorizado a nivel de administrador a un servidor y a la información confidencial que contiene y luego intimida a la víctima amenazando la de divulgar a la prensa a la información si no realiza el pago de un dinero.
- **Uso inapropiado:** Un usuario entrega copias de software de la entidad a personas no autorizadas. Una persona amenaza a otra vía correo electrónico

e. Sistema de información: Cualquier equipo de cómputo o telecomunicaciones, sistema o subsistema interconectado o no conectado usado para la adquisición, almacenamiento, manipulación, gestión, movimiento, control, despliegue, conmutación, intercambio, transmisión o recepción de voz, datos, vídeo en formas análogas o digitales así como el software, firmware o hardware que forme parte del sistema.

6. DESCRIPCIÓN DEL PROCEDIMIENTO

N°	Actividad	Símbolo	Responsable	Punto de Control	Registro
	INICIO	⬭			
1	Registrar el incidente de seguridad de la información.	▭	Grupo de administración de Sistemas		Tiquete de servicio de mesa de ayuda

					Formato de Documentación de Incidentes
2	Analizar e identificar el incidente de seguridad de la información.		Grupo de respuesta a incidentes de seguridad.		Tiquete de servicio de mesa de ayuda (análisis) Formato de Documentación de Incidentes
3	Contener el incidente de seguridad de la información.		Grupo de respuesta a incidentes de seguridad.		Tiquete de servicio de mesa de ayuda (estrategia de contención) Formato de Documentación de Incidentes
4	Erradicar el incidente de seguridad de la información.		Grupo de respuesta a incidentes de seguridad.		Tiquete de servicio de mesa de ayuda (acciones de erradicación) Formato de Documentación de Incidentes
5	Recuperar sistemas afectados		Grupo de respuesta a incidentes de seguridad, Grupo de administración de Sistemas.		Tiquete de servicio de mesa de ayuda (acciones de recuperación) Formato de Documentación de Incidentes
6	Revisión post incidente de seguridad de la información.		Grupo de respuesta a incidentes de seguridad, Grupo de administración de Sistemas.		Tiquete de servicio de mesa de ayuda (lecciones aprendidas) Formato de Documentación de Incidentes Formato de Lecciones Aprendidas Respuesta Incidentes.
	FIN				



7. REGISTROS

- Formato de Documentación de Incidentes
- Formato de Lecciones Aprendidas Respuesta Incidentes

8. CONTROL DE CAMBIOS

VERSIÓN	FECHA	ÍTEM MODIFICADO	DESCRIPCIÓN DEL CAMBIO
01	11/10/2017		