## 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, para prevenir y corregir posibles fallas en la seguridad de la información.

## 2. ALCANCE

Aplica a funcionarios, contratistas, proveedores y terceros con acceso autorizado a los activos de información y medios de procesamiento de información del Instituto para la Economía Social – IPES.

## 3. RESPONSABLES

Es responsabilidad del Comité de Sistemas y Seguridad de la Información del Instituto para la Economía Social - IPES, 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.

## 4. 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:** 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 es cualquier evento que daña o representa una amenaza seria para toda o una



| Elaboró: | Revisó: | Aprobó: |
|---|---|---|
| Yamel Orlando Martínez Balaguera – CPS 134-2019 | John Jair Garzón – Profesional Universitario SDAE | Clarisa Díaz García – Subdirectora de Diseño y Análisis Estratégico |

parte de los medios de procesamiento de información (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, delitos informáticos definidos en la ley 1273 de 2009 u otras normas que cobijen a la entidad.

d) **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.

f) **Administradores de TI:** Personal que hace parte del proceso de gestión de seguridad de la información y recursos tecnológicos, responsables de administrar los activos de infraestructura tecnológica del IPES.

## 5. CONDICIONES GENERALES



| Elaboró: | Revisó: | Aprobó: |
|---|---|---|
| Yamel Orlando Martínez Balaguera – CPS 134-2019 | John Jair Garzón – Profesional Universitario SDAE | Clarisa Díaz García – Subdirectora de Diseño y Análisis Estratégico |

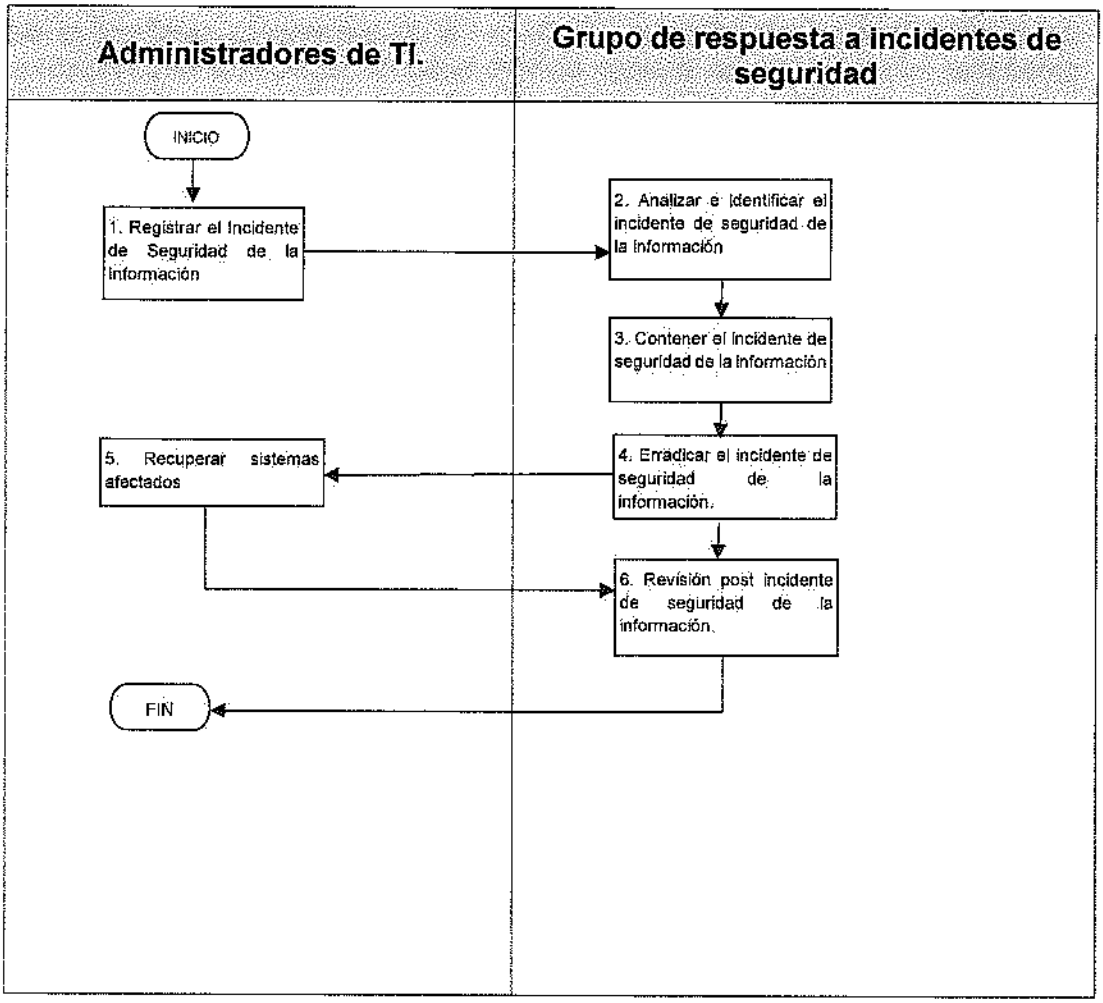
El crecimiento de los sistemas y servicios informáticos que apoyan el cumplimiento de los objetivos y la misión de la entidad, así como el uso de nuevas tecnologías de información y comunicaciones de apoyo en el desarrollo de las actividades institucionales, conllevan a un incremento significativo de 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.

## 6. DESCRIPCIÓN DEL PROCEDIMIENTO






| Elaboró: | Revisó: | Aprobó: |
|---|---|---|
| Yamel Orlando Martinez Balaguera – CPS 134-2019 | John Jair Garzón – Profesional Universitario SDAE | Clarisa Díaz García – Subdirectora de Diseño y Análisis Estratégico |

## 6.1 TABLA EXPLICATIVA DEL PROCEDIMIENTO

| N° | Actividad | Descripción de la actividad | Responsable | Punto de Control | Registro |
|---|---|---|---|---|---|
| | **INICIO** | | | | |
| 1 | Registrar el incidente de seguridad de la información. | Identificar y alertar sobre posibles fallas en la seguridad de la información | Grupo de administración de Sistemas | Diligenciar formato de registro | Tiquete de servicio de mesa de ayuda (estrategia de contención) Formato de FO-625 Documentación de Incidentes |
| 2 | Analizar e identificar el incidente de seguridad de la información. | Evaluar la información ambigua, contradictoria, o incompleta para determinar si está o no ocurriendo un incidente | Grupo de respuesta a incidentes de seguridad. | Documentación del incidente | Análisis de incidentes |
| 3 | Contener el incidente de seguridad de la información. | Estudiar, definir y adoptar la estrategia de contención del incidente | Grupo de respuesta a incidentes de seguridad. | | |
| 4 | Erradicar el incidente de seguridad de la información. | Realizar actividades de erradicación para eliminar los componentes que fueron empleados para el desarrollo del incidente | Grupo de respuesta a incidentes de seguridad. | | |
| 5 | Recuperar sistemas afectados | Restaurar los sistemas y servicios informáticos a su operación normal. | Grupo de respuesta a incidentes de seguridad, Administradores de TI. | Logs de restauración | Logs infraestructura |
| 6 | Revisión post incidente de seguridad de la información. | Seguimiento al comportamiento y estabilidad de los sistemas y servicios informáticos. | Grupo de respuesta a incidentes de seguridad, Administradores de TI. | FO-626 Lecciones aprendidas respuesta a incidentes | Lecciones aprendidas respuesta a incidentes |
| | **FIN** | | | | |



| Elaboró: | Revisó: | Aprobó: |
|---|---|---|
| Yamel Orlando Martinez Balaguera – CPS 134-2019 | John Jair Garzón – Profesional Universitario SDAE | Clarisa Diaz García – Subdirectora de Diseño y Análisis Estratégico |


Página 5 de 6

## 7. DOCUMENTOS ASOCIADOS

MS-013 Manual Subsistema Gestión Seguridad Información
PO-013 Proceso Gestión Seguridad Información y Recursos Tecnológicos
FO-625 Documentación Incidentes
FO-626 Lecciones Aprendidas Respuesta Incidentes
articles-5482_G21_Gestion_Incidentes

## 8. MARCO NORMATIVO

- NTC-ISO/IEC 27001: Tecnología de la Información. Técnicas de Seguridad. Sistemas Gestión de la Seguridad de la Información (SGSI). Requisitos
- NTC-ISO/IEC 27002: Tecnología de la Información. Técnicas de Seguridad. Código de Práctica para la Gestión de la Seguridad de la Información.
- NTD SIG 001:2011: Norma Tecnica Distrital del Sistema Integrado de Gestión para las Entidades y Organismos Distritales.
- Decreto 1499 de 2017 *"Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015*
- Resolución 305 de 2008 Comisión Distrital de Sistemas, por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.

## 9. CONTROL DE CAMBIOS

| VERSIÓN | FECHA | ÍTEM MODIFICADO | DESCRIPCIÓN DEL CAMBIO |
|---|---|---|---|
| 1 | 11/10/2017 | | Elaboración del documento |
| 2 | 31/12/2018 | Objetivo<br>Alcance<br>Responsables<br>Definiciones<br>Condiciones Generales<br>Marco Normativo<br>Se ajusta el formato | Se realizaron cambios en diferentes numerales, ajustando el procedimiento a los accesos físicos a los medios de procesamiento de información. |
| 3 | 28/10/2019 | Tabla Descriptiva | Se ajusta la tabla descriptiva estableciendo los puntos de control. |



| Elaboró: | Revisó: | Aprobó: |
|---|---|---|
| Yamel Orlando Martinez Balaguera – CPS 134-2019 | John Jair Garzón – Profesional Universitario SDAE | Clarisa Díaz García – Subdirectora de Diseño y Análisis Estratégico |

Página 6 de 6