ALCALDÍA MAYOR
DE BOGOTÁ D.C.
DESARROLLO ECONÓMICO
Instituto para la Economía Social

IPES

GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

SUBDIRECCION DE DISEÑO Y ANÁLISIS ESTRATÉGICO

Bogotá 2017

Tabla de contenido

1 OBJETIVO

Establecer los métodos estándar para identificar, realizar seguimiento y responder a los incidentes de seguridad de la información del INSTITUTO PARA LA ECONOMIA SOCIAL.

2 ALCANCE

Aplica a funcionarios, contratistas, proveedores y todo personal que tenga acceso a recursos de información y tecnología del INSTITUTO PARA LA ECONOMIA SOCIAL, así como a todos los recursos de información y tecnología empleados para la prestación de servicios de la entidad.

3 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 gestión de incidentes de seguridad de la información, actualizarlo y evaluar las acciones de mejora que se identifiquen del tratamiento de los incidentes de seguridad que sean detectados.

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 DEFINICIONES Y ABREVIATURAS

a) 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 o 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.

b) Incidente de seguridad: Un incidente de seguridad de la información es cualquier evento que puede dañar o representa una amenaza seria para toda o una parte de la infraestructura tecnológica y activos de información del INSTITUTO PARA LA ECONOMIA SOCIAL (sistemas de cómputo, sistemas de información, red de datos), como pueden ser: ausencia de servicios, indisponibilidad de los 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.

c) Incidente de seguridad computacional: Un incidente de seguridad computacional es una violación o potencial amenaza de violación[1] 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 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.

d) Sistema de información: Cualquier equipo de cómputo o telecomunicaciones, sistema o subsistema interconectado o no conectado usado para la adquisición, almacenamiento, manipulación, gestión,

[1] Una inminente amenaza de violación se refiere a una situación en la cual la entidad tiene una base cierta para creer que un incidente esta por ocurrir. Por ejemplo: El administrador del software de antivirus recibe un boletín del fabricante del software donde le informa que un nuevo tipo de virus está circulando a gran velocidad por internet.

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 MANEJO DE INCIDENTES

El manejo de los incidentes de seguridad de la información en el INSTITUTO PARA LA ECONOMIA SOCIAL, sigue los requerimientos de la norma NIST-800-61 Computer Security Incident Handling Guide (http://www.nist.gov) y la norma ISO18044 gestión de incidentes de seguridad de la información.

Las etapas del procedimiento de atención de incidentes de seguridad de la información incluyen:

- Preparación
- Detección y análisis
- Contención, Erradicación y recuperación
- Revisión post incidente

6.1 Resumen ejecutivo del procedimiento

Durante la etapa de preparación la entidad debe procurar reducir el número de incidentes que pueden ocurrir mediante la selección e implementación de controles basados en los resultados de la evaluación de riesgos del sistema de gestión de seguridad de la información, sin embargo es importante ser consciente que existe una porción de los riesgos que no puede ser cubierta por los controles implementados y que se denomina riesgo residual.

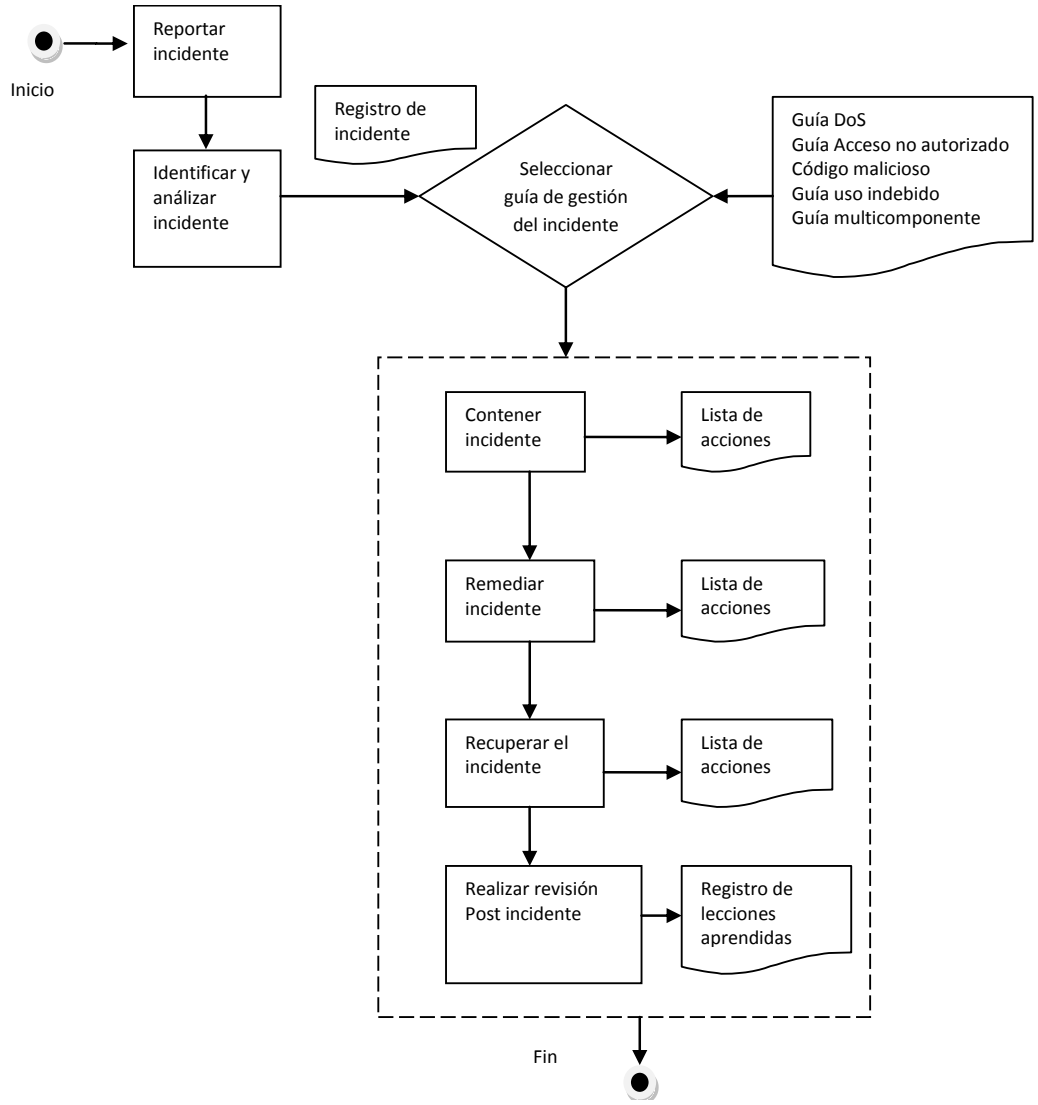
En la etapa de detección es necesario alertar a la entidad de la ocurrencia de un incidente y de acuerdo con la severidad del incidente se debe actuar para mitigar el impacto del mismo mediante acciones de contención y remediación.

Después de que el incidente ha sido apropiadamente gestionado, se debe emitir

un reporte que detalle las causas, costos del incidente y pasos que se seguirán para prevenir futuros incidentes.

A continuación se describen en detalle las actividades de las etapas de: preparación, detección y análisis, contención, erradicación, recuperación y revisión post incidente.

FLUJOGRAMA DE GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN



6.2 Preparación

6.2.1 Introducción

La etapa de preparación es fundamental no solo para que la entidad este en capacidad de gestionar incidentes de seguridad, sino también para que prevenga su ocurrencia mediante el aseguramiento de sus sistemas y servicios informáticos.

Aunque la preparación no es propiamente una etapa de las actividades que se realizan cuando se presentan los incidentes, es necesario realizar actividades de prevención y mejora continua para reducir la posibilidad de ocurrencia o mitigar los impactos de los incidentes de seguridad.

6.2.2 Preparación para la gestión de incidentes

En el anexo A *LISTA DE CHEQUEO DE HERRAMIENTAS PARA ATENCIÓN DE INCIDENTES DE SEGURIDAD* se describen herramientas que permiten estar preparado para realizar una apropiada gestión de incidentes. El Comité de Sistemas y Seguridad de la Información del INSTITUTO PARA LA ECONOMIA SOCIAL, debe procurar la aplicación de los aspectos definidos, a fin de contar con las herramientas necesarias para gestionar los incidentes de seguridad.

Adicionalmente se debe preparar un kit de atención de incidentes que pueda ser transportado por los miembros del equipo de atención de incidentes. El kit debe contener elementos como: Laptop con el software de atención de incidentes precargado (sniffer, software forense), medios de backup, medios para imagen forense, cables, medios de almacenamiento en blanco, copias de sistemas operacionales. El kit debe permanecer disponible, actualizado y completo para cuando sea requerido.

6.2.3 Prevención de incidentes

Con el fin de alcanzar niveles apropiados de seguridad de la información en la entidad, es necesario mantener el número de incidentes de seguridad en escalas razonables. Es importante mantener una cultura de prevención que reduzca el número de incidentes que demanden la intervención del equipo de gestión de incidentes, por esa razón es necesario realizar, a intervalos periódicos, análisis de seguridad para identificar fuentes de riesgo y diseñar controles que reduzcan la posibilidad de ocurrencia de los incidentes. Las actividades de gestión de riesgos se deben realizar empleando la metodología de gestión de riesgos de seguridad adoptada por la entidad.

Algunas acciones particulares que se deben evaluar para mitigar la ocurrencia de incidentes de seguridad son:

- Administración de parches
- Aseguramiento de servidores
- Seguridad de redes
- Previsión de código malicioso
- Entrenamiento y toma de conciencia en seguridad de la información

6.3 Detección y análisis

6.3.1 Introducción

Los incidentes pueden ocurrir por múltiples causas, por esa razón resulta poco práctico desarrollar procedimientos detallados (paso a paso) de cada uno de los tipos de incidentes que podrían presentarse, por esa razón el IPES ha adoptado un procedimiento general que cubre las etapas mínimas que se deben seguir en la atención de incidentes, para algunos casos particulares se definen acciones específicas que se detallaran en otras secciones del presente instructivo.

6.3.2 Clasificación de los incidentes

La siguiente clasificación ilustra las agrupaciones que se darán a los tipos de incidentes, esta clasificación se emplea para normalizar las actividades de gestión de los incidentes y la generación de estadísticas.

- **Categoría 1 Acceso no autorizado**: Se califican los incidentes donde un agente (interno o externo, persona o sistema), gana acceso lógico o físico a un recurso de información y tecnología (equipo, dato, software, red, etc.) sobre el cual no tiene derechos.

- **Categoría 2 Denegación de servicio:** Se califica en esta categoría incidentes en los cuales un atacante (interno o externo a la entidad) impide el uso autorizado de servicios informáticos, redes o sistemas de información mediante el consumo excesivo de recursos de la plataforma o sistema bajo ataque.

- **Categoría 3 Código malicioso**: En esta categoría están los incidentes en donde software como virus, troyanos, RAT, Rootkit, Ransomware, gusanos y demás formas de código malicioso infectan exitosamente un recurso de información y tecnología del Instituto para la Economía Social.

- **Categoría 4 Uso inapropiado**: Se presenta cuando las partes interesadas (interno o externo, persona o sistema) incumplen la política de seguridad de la información institucional.

- **Categoría 5 Multicomponente**: Son incidentes en los cuales se presentan más de una de las formas de incidentes antes descritos.

Las anteriores categorías son una vista de las categorías aprobadas por el *US-CERT Incident Categories and Reporting Timeframes,* se excluyeron de las categorías los incidentes relacionados con ejercicios militares. Para mayor información consultar NIST 800-61 Anexo J.

6.3.3 Síntomas de un incidente

Debido a que la tarea más compleja en el proceso de respuesta a un incidente es identificar si se va a presentar o se está presentando, es necesario que el oficial o de seguridad de la información (designado por el comité de sistemas y seguridad e la información) tenga en cuenta los siguientes factores que dificultan dicha labor:

- Los incidentes pueden ser detectados por diferentes medios los cuales varían en el nivel de detalle y fidelidad. Las herramientas automáticas pueden incluir, sistemas de detección/prevención de intrusos, software de antivirus o analizadores de logs. Los incidentes también pueden ser detectados por medios manuales como reportes de problema de los usuarios. Aunque existen incidentes que pueden ser detectados fácilmente existen otros que no se detectan hasta que sus efectos son notorios.

- El volumen de síntomas potenciales de un incidentes por lo regular es alto, por ejemplo un IDS puede generar miles de falsos positivos, por esa razón es necesario filtrar apropiadamente la información proveniente de herramientas automáticas.

- Se requiere conocimiento especializado y experiencia para realizar análisis detallados de la información recolectada durante la identificación de un incidente**.**

Los síntomas de los incidentes se pueden clasificar en dos categorías: Precursores e indicadores.

Precursor: Es un síntoma que indica que el incidente puede ocurrir en el futuro.
Indicador: Es un síntoma que indica que el incidente ha ocurrido o está ocurriendo.

Debido a que existen múltiples fuentes que pueden identificar un precursor o indicador, a continuación se relacionan síntomas comunes que debe supervisar periódicamente el oficial o encargado de seguridad de la información.

Fuente de precursor o indicador	Descripción
Software de antivirus, antispyware, Antispam.	Cuando el software de antivirus o antispyware detecta código malicioso típicamente genera alertas. Si las firmas digitales de código malicioso del software de antivirus y antispyware están actualizadas, el mismo software puede aislar y erradicar el código malicioso. El software de control de código malicioso debe ser verificado para la plataforma perimetral y a nivel de los servidores. El software antispam se emplea para detectar y prevenir la llegada de correo no deseado a los buzones de los usuarios. El software de antispam debe estar actualizado para detectar y contener malware o phishing, el oficial o encargado de seguridad de la información debe verificar periódicamente los reportes de estas herramientas de prevención de incidentes.
Software de verificación de integridad.	El software de verificación de integridad permite detectar cambios en el checksum de archivos clave de los servidores, la verificación periódica de los reportes del software de verificación de integridad permite la identificación de incidentes potenciales.
Software de monitoreo.	El software de monitoreo de plataforma verifica a intervalos periódicos el funcionamiento de los servicios y la plataforma de tecnología, cuando el servicio o recurso no responde o presenta un comportamiento fuera de lo común se deben verificar las alertas para descartar ocurrencia de incidentes.
Registros	
Registros del sistema operacional y las aplicaciones.	Los registros de los sistemas operacionales y especialmente de los de auditoría son de gran valor para la identificación de incidentes, los registros no se deben deshabilitar, se debe preservar y el comportamiento rutinario de los servicios se debe establecer para detectar cambios que sean signos de la posible ocurrencia de incidentes de seguridad de la información.
Registros de los servicios de red.	Por lo general los registros de firewall o *routers* no constituyen fuente primaria de precursores o indicadores debido a que por lo regular se configuran para grabar conexiones bloqueadas y proporcionan poca información sobre el comportamiento de un incidente, sin embargo el encargado de seguridad de la

	información debe verificar esto registros para identificar patrones de comportamiento en acceso a puertos de la red.
Bases de datos de amenazas y vulnerabilidades.	El encargado de seguridad de la información debe verificar periódicamente las bases de datos de vulnerabilidades y amenazas para identificar indicadores de incidentes que puedan afectar a la entidad y prepararse para afrontar futuros ataques. Las bases de datos que se debe verificar con regularidad son US-CERT y CERT /CC
Informes de incidentes de otras entidades	El oficial o encargado de seguridad de la información de la entidad debe mantener contacto con los centros de respuesta a incidentes del gobierno colombiano y la comisión distrital de sistemas de la alcaldía de Bogotá. También se debe mantener contacto con grupos de interés en seguridad de la información ej, SEGURINFO.
Personal de INSTITUTO PARA LA ECONOMIA SOCIAL y otras organizaciones	
Funcionario /contratistas del INSTITUTO PARA LA ECONOMIA SOCIAL	Los usuarios, administradores de sistemas, administradores de red, miembros de los equipos de gestión de incidentes y en general todas las personas que hagan uso de servicios o recursos del IPES, debe reportar síntomas de incidentes de seguridad.
Personal de otras entidades u organizaciones	Aunque muy pocos incidentes de seguridad podrían ser reportados por personal externo a la entidad, esos reportes deben ser evaluados y tomados en consideración.

6.4 Análisis del incidente

La detección y análisis de los incidentes se simplifica cuando el precursor o el indicador se identifican con precisión, sin embargo no siempre se pueden identificar con precisión esos factores. Es responsabilidad del grupo de gestión de incidentes la evaluación de la pertinencia de los síntomas detectados y actuar de conformidad, en general los responsables de la gestión de incidentes deben asumir que el incidente está ocurriendo hasta que se confirme que no ocurre nada. Los responsables de la gestión de incidentes deben analizar información ambigua, contradictoria o incompleta para determinar si está o no ocurriendo un incidente.

El grupo de gestión de incidentes debe trabajar con prontitud para analizar y validar cada incidente y documentar desde la fase de identificación del incidente cada paso que se realice para su tratamiento.

Cuando el grupo de gestión de incidentes considere que está ocurriendo un incidente, se debe realizar un análisis rápido para determinar el alcance del incidente (redes, sistemas o aplicaciones afectadas), quién o cual es la fuente del incidente, cómo está ocurriendo el incidente (herramientas que se están usando para realizar el ataque, vulnerabilidades que están explotando). El análisis inicial del incidente debe contener información suficiente para priorizar las siguientes actividades de manejo del mismo.

Las siguientes recomendaciones se deben tener en cuenta al momento de realizar el análisis inicial del incidente:

- Perfiles de redes y sistemas: Se deben mantener perfiles o registros actualizados del comportamiento de los diferentes dispositivos y sistemas, de esa forma se puede predecir el comportamiento de los mismos e identificar comportamientos no esperados o irregulares.

- Comprensión del comportamiento normal: Se deben estudiar periódicamente las redes, sistemas y aplicaciones para obtener un conocimiento detallado de lo que se considera un comportamiento normal y así identificar comportamientos anormales y reconocer fácilmente la ocurrencia de incidentes.

- Uso de log centralizado y política de retención de registros: Los registros de los diferentes dispositivos de red, sistemas de información y servicios se deben consolidar en uno o puntos únicos de recolección centralizados y mantener copias de los mismos para facilitar el análisis de los incidentes. De igual forma se deben cumplir las políticas de retención de registros de comportamiento de los sistemas y dispositivos de infraestructura de información y tecnología.

- Realizar correlación de eventos: Debido a que los incidentes pueden implicar a varios recursos de información y tecnología, el equipo de atención de incidentes debe utilizar herramientas de software que les permitan realizar la correlación de los registros generados por cada uno de los dispositivos, sistemas y servicios implicados en el incidente.

- Mantener los relojes de los sistemas sincronizados con una fuente única: Para que el proceso de correlación de eventos sea efectivo es necesario

mantener sincronizados los relojes de los diferentes dispositivos y sistemas, se debe usar como fuente de sincronización la hora legal colombiana emitida por la superintendencia de industria y comercio.

- Mantener y usar una base de conocimiento: El equipo de respuesta a incidentes debe mantener registros de las lecciones aprendidas del manejo de incidentes, esta base de conocimiento se puede elaborar en hojas electrónicas o bases de datos que faciliten la recopilación de información como:

  - Enlaces a información sobre códigos maliciosos y Hoax.
  - Explicaciones y detalles de indicadores y precursores de incidentes de seguridad tales como alertas de detección de intrusos, registros de entrada a sistemas operacionales y códigos de error de aplicaciones.
  - Lista de dominios reportados en listas negras por envío de spam.

- Uso de motores de búsqueda en internet: La consulta de información en motores de búsqueda como Google y bing, pueden ayudar al análisis de los incidentes de seguridad de la información. Otras fuentes son las listas de correo especializadas en seguridad de la información en donde se mantienen archivos históricos.

- Ejecutar *sniffers* para recolectar información complementaria: Cuando los indicadores del incidente no registran información suficiente en los dispositivos se debe utilizar software como *sniffers* para recopilar información en toda la red.

- Filtrado de datos: Debido a que durante un incidente se pueden generar un elevado volumen de datos que impiden su análisis total y detallado, el equipo de respuesta a incidentes debe filtrar la información recolectada para facilitar el análisis de los datos. El equipo de respuesta a incidentes debe identificar los mejores criterios de filtrado de datos de acuerdo con la naturaleza particular de cada incidente.

- Basarse en la experiencia para analizar los indicadores y precursores: La mejor forma de identificar un incidente es ganar tanta experiencia como sea posible en los procesos de respuesta a incidentes. El equipo de respuesta incidentes debe compartir periódicamente los hallazgos realizados y la experiencia en análisis de datos de la gestión de incidentes anteriores.

- Elaborar matrices de diagnóstico para los miembros menos experimentados

del equipo: La información de diagnóstico de incidentes debe estar disponible en formatos comprensibles para los grupos de mesa de ayuda, administradores y otras personas que participen en las actividades de respuesta a riesgos.

- Búsqueda de asistencia externa: Cuando el equipo de respuesta a incidentes requiera apoyo externo, debe realizar el escalamiento con el comité de sistemas y seguridad de la información para coordinar apoyo de centros de respuesta a incidentes de la Alcaldía de Bogotá, Policía Nacional o ministerio de Defensa nacional.

6.4.1 Documentación del incidente.

Una vez que el equipo de respuesta a incidentes sospeche que un incidente está ocurriendo u ocurrió, se debe iniciar la documentación del mismo. Es necesario documentar únicamente los hechos relacionados con el incidente, se debe evitar el registro de opiniones personales o subjetivas. El anexo B del presente instructivo contiene un formato de registro de hechos del incidente.

Los miembros del equipo de gestión de incidentes debe llevar registro de las acciones ejecutadas para la atención del incidente, el registro de debe llevar en una bitácora de seguimiento del incidente, el mecanismo más simple es el uso de una libreta de anotaciones, pero también se puede usar computador personal, Smartphone u otro tipo de tecnología que permita llegar registro de las actividades. Las notas de las acciones ejecutadas se deben transcribir en limpio. Las notas originales no deben ser destruidas, borradas o alteradas, no se deben retirar hojas de los cuadernos de notas o borrar las anotaciones realizadas en equipos electrónicos. Todas las notas deben quedar firmadas y fechadas por el autor**.** Todas las notas realizadas pueden constituir evidencias en procesos legales. Las diferentes actuaciones del equipo de respuesta a incidentes deben registrarse en la mesa de ayuda. Los datos que los miembros del equipo de respuesta a incidentes deben registrar incluyen:

- Estado actual del incidente
- Resumen del estado actual del incidente
- Acciones que se han tomado para dar respuesta al incidente
- Información de contacto de las personas que se han involucrado en el incidente
- Lista de la evidencia recolectada a la fecha
- Siguientes pasos que se deben realizar

El equipo de respuesta a incidentes debe preservar toda la información de las acciones y evidencias recolectadas durante el proceso de atención del incidente debido a que muchas veces contiene información sensible como: vulnerabilidades no detectadas, acciones indebidas realizadas por usuarios o atacantes, brechas de seguridad en los sistemas o la plataforma tecnológica. Los correos, documentos, y reportes relacionados con el manejo del incidente deben ser cifrados para evitar acceso no autorizado a los mismos.

6.4.2 Priorización del incidente

Todos los incidentes deben ser priorizados para garantizar que son atendidos de acuerdo con su nivel de criticidad. Para todos los incidentes se debe evaluar los siguientes factores:

- Efectos técnicos reales y potenciales del incidente
- Recursos críticos afectados por el incidente

Los incidentes que impactan directamente la continuidad de las actividades misionales de la entidad requieren atención prioritaria.

La primera tarea para priorizar los incidentes es calificar el nivel de los efectos. La siguiente tabla permite establecer el nivel de efectos del incidente.

Cuantificación de efectos (reales o proyectados)

Valor	Escala cualitativa del efecto	Descripción
0.0	Ninguno	No se afectan sistemas críticos, No se afectan múltiples áreas.
0.10	Mínimo	Efectos imperceptibles (no los nota ningún área de la entidad)
0.25	Bajo	Efectos moderados (los nota el área afectada pero el trabajo puede continuar)
0.50	Medio	Efectos severos en un área de la entidad o efectos imperceptibles en varias áreas o efectos imperceptibles en un recurso crítico
0.75	Alto	Efectos moderados en múltiples áreas del INSTITUTO PARA LA ECONOMIA SOCIAL o efectos moderados en un recurso crítico (el recursos o servicio trabaja de manera degradada)
1.0	Crítico	Efectos severos en varias áreas del INSTITUTO PARA LA ECONOMIA SOCIAL (no se puede continuar

Valor	Escala cualitativa del efecto	Descripción
		trabajando) o efectos severos en un recurso crítico (no puede prestar servicios)

Después de aplicar la tabla de valoración de efectos se debe asignar un nivel de criticidad a los sistemas afectados.

Cuantificación de criticidad

Valor	Escala cualitativa de criticidad	Descripción
0.10	Mínimo	No es un sistema crítico o componente de infraestructura (verificar usando el plan de contingencia de IT los sistemas críticos)
0.25	Bajo	Sistema o componente que apoya la operación de un (1) área del INSTITUTO PARA LA ECONOMIA SOCIAL
0.50	Medio	Sistema o componente que apoya la operación de más de un área del INSTITUTO PARA LA ECONOMIA SOCIAL
0.75	Alto	Sistema o componente crítico que soporta la operación de un área del INSTITUTO PARA LA ECONOMIA SOCIAL
1.0	Critico	Sistema o componente que soporta la operación misional de todas las áreas del INSTITUTO PARA LA ECONOMIA SOCIAL

Para determinar el nivel de severidad del incidente se debe calcular la siguiente formula

Sever = Nivel de efecto real * 2.5 + nivel de efecto potencial* 2.5 +Criticidad del sistema* 5

Una vez realizado el cálculo el incidente recibe el nivel de impacto de acuerdo con la siguiente tabla, los incidentes se deben atender en orden de prioridad de acuerdo con su nivel de impacto: En primera instancia siempre los incidentes críticos y en última instancia los de impacto ninguno

Ranking de impacto de incidente

Calificación	Nivel de impacto
0.00 a 00.99	Ninguno
01.00 – 02.49	Mínimo
02.50 – 03.74	Bajo
03.75 – 04.99	Medio
05.00 – 07.49	Alto
07.50 – 10.00	Crítico

6.4.3 Notificación del incidente

Una vez que el incidente ha sido analizado y priorizado se debe proceder a notificar a las instancias e individuos apropiados y en los casos que determine el [jefe del área de sistemas de la entidad]

Las personas que deben ser notificadas de los incidentes de acuerdo con el nivel de escalamiento que reciba el incidente incluyen:

El oficial o encargado de seguridad de la información
El jefe del área de sistemas del INSTITUTO PARA LA ECONOMIA SOCIAL
El jefe de la oficina de control interno
El jefe de la oficina jurídica
El director del INSTITUTO PARA LA ECONOMIA SOCIAL
Equipo de atención de incidentes de la comisión Distrital de sistemas
Equipo de atención de incidentes de la policía nacional
Equipo de atención de incidentes del ministerio de defensa

De acuerdo con el análisis del incidente el equipo de respuesta a incidentes debe determinar la frecuencia y métodos a emplear para generar reportes periódicos sobre el estado de avance en la atención de incidentes. Los métodos incluyen:

- Correo electrónico (si está disponible y es seguro su uso)
- Llamada telefónica
- En persona
- Papel

6.4.4 Clasificación de estado actual del incidente

Debido a que se deben mantener informadas a las partes pertinentes sobre la evolución del incidente, la siguiente tabla describe los estados definidos para los incidentes.

Estado	Descripción

Estado	Descripción
Pendiente	Si bien el incidente ha sido reportado, aún no se lo ha comunicado al [oficial o encargado de Seguridad de la información]
Informado	El incidente ha sido reportado al [oficial o encargado de Seguridad de la información] pero aún no se lo ha tratado
En curso	El incidente ha sido reportado al [oficial o encargado de Seguridad de la información] y se encuentra en tratamiento
Resuelto	El incidente ha sido resuelto
Demorado	El tratamiento ha sido interrumpido por motivos a detallar

6.5 Contención, erradicación y recuperación del incidente

6.5.1 Selección de la estrategia de contención

Una vez analizado y priorizado el incidente se debe contener su acción para evitar que su propagación impida su erradicación y afecte a otros sistemas. Las posibles acciones de contención deben ser analizadas por el equipo de atención de incidentes. Cada incidente tiene su forma particular de contención que debe ser estudiada, definida y adoptada por el equipo de respuesta a incidentes, algunas de las opciones de contención incluyen:

- Apagar el sistema afectado
- Desconectar el sistema de redes alambradas o inalámbricas
- Deshabilitar funciones del sistema
- Apagar servicios

Como guía de trabajo los anexos C, D, E, F y G indican posibles acciones para cada tipo de incidente, es responsabilidad del equipo de respuesta a incidentes determinar la estrategia según el tipo de incidente.

Anexo C: Manejo de incidentes de denegación de servicios
Anexo D: Manejo de incidentes de código malicioso
Anexo E: Manejo de incidentes de acceso no autorizado
Anexo F: Manejo de incidentes de uso inapropiado
Anexo G: Manejo de incidentes multicomponente

Los anexos mencionados anteriormente son guías que apoyaran el trabajo del equipo de atención de incidentes, pero siempre se debe priorizar la atención del incidente considerando criterios como:

- Daño potencial y pérdida de recursos
- Necesidad de preservación de evidencias
- Disponibilidad del servicio
- Tiempo y recursos necesarios para implementar la estrategia de manejo del incidente
- Efectividad de la estrategia seleccionada
- Duración de la solución

6.5.2 Recolección y manejo de evidencias

Aunque la razón principal para la recolección de evidencias es la gestión del incidente también es necesaria para eventuales procesos legales. Se debe seguir los procedimientos de recolección y manejo de evidencias forenses del INSTITUTO PARA LA ECONOMIA SOCIAL, la evidencia debe ser recolectada cumpliendo la regulación y recomendaciones del área jurídica del INSTITUTO PARA LA ECONOMIA SOCIAL de forma que sea admisible en procesos legales.

6.5.3 Manejo forense de computadores

A continuación se resumen las recomendaciones generales para la recolección de evidencias en computadores. Es indispensable seguir procedimientos forenses aprobados para poder recolectar evidencias validas en procesos legales.

Antes de generar las imágenes forenses se deben recolectar los datos volátiles que no quedarán registrados en los filesystem del sistema afectado. La información volátil incluye pero no se limita a: conexiones de red activas, procesos en ejecución, registros de sesiones activas, archivos abiertos, configuración de las interfaces de red y contenidos de memoria.

Es necesario tener en cuenta que cualquier acción que se ejecute sobre el servidor puede afectar sustancialmente las evidencias, de igual forma el atacante puede estar aún dentro del equipo y la recolección de la evidencia en esas circunstancias puede tener consecuencias técnicas irreparables para el equipo y la información.

Es indispensable que las actividades de recolección de la evidencia sean realizadas por personal debidamente entrenado y que se emplee el mínimo de comandos para evitar la modificación de la evidencia.

Finalizada la captura de la información volátil se debe proceder con la obtención de la imagen forense del equipo afectado, se deben realizar no menos de dos imágenes forenses que se deben rotular y almacenar en lugar seguro bajo cadena de custodia las cuales deben ser usadas estrictamente como evidencias ***(toda evidencia debe ser etiquetada y almacenada en forma segura, eso incluye***

imágenes forenses y todos los demás tipos de evidencias). Ocasionalmente puede ser necesario asegurar el disco original. Además de la imagen forense del equipo afectado es necesario recolectar evidencias generadas de otros dispositivos como firewall, DNS los registros de estos dispositivos también deben ser almacenados es dispositivos de solo lectura, la segunda copia de esos registros puede ser empleada para análisis del incidente.

6.5.4 Manejo forense de dispositivos móviles

El manejo forense de dispositivos móviles como smartphones implica el uso de equipo especializado, conocimiento y procedimientos específicos. Lo ideal es que el equipo de respuesta a incidentes solicite apoyo especializado para el manejo de este tipo de evidencias.

6.5.5 Identificación del atacante

Durante el manejo del incidente el equipo de respuesta a incidentes puede querer identificar atacante, si bien esta información puede ser valiosa para el Fondo de Vigilancia en procesos legales.

La prioridad del grupo de respuesta a incidentes debe ser la contención erradicación y recuperación del incidente

La identificación del atacante es una actividad que consume mucho tiempo y que desvía la atención del grupo de respuesta a incidentes del restablecimiento de los servicios afectados. Si el [oficial o encargado de seguridad de la información] autoriza la identificación del atacante se deben considerar:

- Validación de la dirección IP del atacante
- Explorar el sistema del atacante
- Recolectar evidencias del atacante mediante motores de búsqueda
- Usar bases datos de incidentes
- Supervisar los posibles canales de comunicación del atacante

6.6 Erradicación y Recuperación

Después de que el incidente ha sido contenido es necesario realizar actividades de erradicación para eliminar los componentes que fueron empleados para el desarrollo del mismo, las acciones pueden incluir eliminar el código malicioso y remover cuentas de usuario creadas por el atacante. En algunos ataques la erradicación no es necesaria o se realiza durante las actividades de recuperación. En la fase de recuperación los administradores restauran los sistemas a su operación normal, si aplica se realiza endurecimiento (*hardenning*) de los equipos para prevenir acciones futuras.

6.7 Seguimiento post incidente

6.7.1 Lecciones aprendidas

De cada incidente de seguridad se debe realizar un aprendizaje que permita identificar las amenazas, vulnerabilidades y oportunidades de mejora. La ejecución de una reunión en donde se estudien y documenten las lecciones aprendidas derivadas de la atención del incidente es una de las herramientas más útiles para la mejora en los procesos de atención de incidentes de seguridad de la información. A continuación se relaciona un conjunto de preguntas que sirven como guía para el desarrollo de la reunión de lecciones aprendidas:

- ¿Exactamente qué sucedió?
- ¿Fue bueno el desempeño del grupo de atención de incidentes y del grupo directivo del INSTITUTO PARA LA ECONOMIA SOCIAL?
- ¿Se siguieron los procedimientos documentados?
- ¿Fueron adecuados los procedimientos?
- ¿Se ejecutaron pasos o acciones que pudieron impedir la recuperación?
- ¿Qué acciones se deben ejecutar en forma diferente durante la atención de un futuro incidente?
- ¿Qué herramientas adicionales o recursos son necesarias para detectar, analizar, y mitigar futuros incidentes?

El resultado de la reunión de lecciones aprendidas se debe documentar en el registro de lecciones aprendidas.

6.7.2 Generación de estadísticas de los incidentes

La recolección de datos sobre el desempeño del grupo de respuesta a incidentes es una herramienta de gran valor para el mejoramiento continuo de la gestión de incidentes. Los datos estadísticos permitirán identificar debilidades en la atención de incidentes, esas debilidades deben ser usadas en el proceso de gestión de riesgos. Dentro de la información estadística que se debe recolectar se encuentra:

- Número de incidentes atendidos por mes: La atención de un elevado número de incidentes no necesariamente es un buen indicador, es posible que no se están evaluando correctamente las vulnerabilidades existentes. La existencia de pocos incidentes atendidos tampoco es un mal indicador, es posible que las medidas preventivas hayan sido efectivas.
- Tiempo empleado en la atención de incidentes: respecto a cada incidente debe documentarse:
- Tiempo total invertido para responder al incidente.
- Tiempo transcurrido desde la identificación del incidente y su erradicación
- Tiempo invertido en cada una de las etapas de atención del incidente

(análisis, contención, erradicación)
- Tiempo que tomo al grupo de respuesta iniciar la atención del incidente
- Tiempo transcurrido desde la detección del incidente y su reporte [al nivel directivo del INSTITUTO PARA LA ECONOMIA SOCIAL]

6.7.3 Evaluación objetiva del incidente.

Determinar cuál o cuáles de las acciones de respuesta a incidente fueron más efectivas. Dentro de las acciones a evaluar se deben considerar:

- Revisión de registros (logs), reportes y documentación complementaria que determinará la estrategia de respuesta al incidente
- Identificación de precursores e indicadores que facilitaron la detección y registro del incidente
- Determinación de si el incidente causó daños antes de su identificación
- Determinación de si la causa raíz del incidente fue verdaderamente identificada
- Cálculo del valor monetario estimado del daño
- Identificación de que medidas hubieran prevenido el incidente

6.7.4 Lista de chequeo de atención de incidentes de seguridad de la información

A continuación se detalla la lista de actividades que se deben verificar y documentar al momento de realizar la atención de los incidentes de seguridad, la lista está orientada a las actividades de atención inicial del incidente, el grupo de respuesta a incidentes debe usar las listas de chequeo especificas descritas en los anexos C al G de acuerdo con el tipo específico de incidente.

Detección y análisis		
Paso	**Acción**	**Ejecutada?**
1	Determinar si ha ocurrido un incidente	
1.1	Analizar los precursores e indicadores	
1.2	Buscar correlación de eventos	
1.3	Realizar investigación en Internet	
1.4	Documentar a la mayor brevedad las acciones de respuesta	
2	Clasificar el incidente usando las categorías definidas	
3	Seguir los pasos apropiados para responder ante el incidentes apoyándose en la los anexos C al G. Si el incidente no concuerda con ninguna categoría identificada usar la lista genérica de atención de incidentes	

Lista genérica de respuesta a incidentes no categorizados		
Paso	**Acción**	**Ejecutada?**
1	Priorizar la atención del incidente de acuerdo con el impacto para la entidad	
2	Identificar que recursos han sido afectados y cuáles podrían ser afectados	
3	Estimar el impacto técnico del incidente	
4	Calcular la prioridad del incidente de acuerdo con las matrices definidas	
5	Reportar el incidente a las instancias competentes(internas o externas si aplica)	
Contención, Erradicación y recuperación		
Paso	**Acción**	**Ejecutada?**
1	Recolectar, preservar y asegurar las evidencias	
2	Contener el incidente	
3	Erradicar el incidente	
3.1	Identificar y mitigar todas las vulnerabilidades que se explotan	
3.2	Remover el código malicioso, material inapropiado y otros componentes	
4	Recuperarse del incidente	
4.1	Restaurar los sistemas a su estado operativo	
4.2	Confirmar que los sistemas afectados están funcionando correctamente	
4.3	Si es necesario implementar medidas adicionales de supervisión	
Revisión post incidente		
Paso	**Acción**	**Ejecutada?**
1	Crear reporte de atención del incidente	
2	Realizar reunión de lecciones aprendidas	

ANEXO A
LISTA DE CHEQUEO DE HERRAMIENTAS PARA ATENCIÓN DE INCIDENTES DE SEGURIDAD

Completo?	Herramienta
Elementos de comunicación	
	Información de contactos de los miembros del equipo de atención de incidentes y otras personas dentro y fuera de la entidad (contacto primario y contacto alterno) que pueden servir como apoyo en el manejo del incidente: Técnicos, Abogados, representantes de organismos de seguridad.
	Mecanismo para reporte de incidentes Definición de los mecanismos que se emplearan para el reporte de incidentes, teléfonos, correos electrónicos, formatos online que puedan utilizar los usuarios para reportar los posibles incidentes [deseable contar con un mecanismo para recibir reportes de manera anónima]
	Teléfonos celulares o radios de comunicaciones Disponer de teléfonos o radios que sean portados por los miembros del equipo de gestión de incidentes en horas de oficina y fuera del horario de trabajo. [deseable contar con un teléfono o radio de servicio que pueda ser rotado por el ingeniero de servicio en horas no hábiles]
	Área de manejo de crisis Oficina desde la cual se puedan gestionar de manera centralizada las actividades de manejo del incidente. [si no se cuenta con un área permanente se debería definir un mecanismo para reservar una oficina cuando se requiera la atención de incidentes]
	Área de almacenamiento de evidencias Área física en donde se almacenaran, preservaran y custodiarán las evidencias que se recolecten durante el manejo del incidente.
Software y hardware para manejo de incidentes	
	Estaciones de computación forense y dispositivos para backup
	Computadores portátiles
	Estaciones de trabajo para montaje de un laboratorio para pruebas de herramientas forenses. [si no se cuenta con estaciones suficientes se pueden establecer acuerdos o contratos para tener disponibilidad de laboratorios forenses bajo demanda]
	Medio de almacenamiento (CD, DVD, *BlueRay*, discos USB, discos externos)

	Impresora portátil. Para imprimir evidencias de equipos que no estén conectados a la red
	Analizadores de protocolos o *sniffer*
	Software de computo forense
	Accesorios para recolección de evidencias (cámaras digitales, grabadoras de audio, formatos de cadena de custodia, bolsas y etiquetas para almacenar evidencias, discos para imagen forense)
Recursos para análisis de incidentes	
	Lista de puertos (especialmente los usados por malware)
	Documentación de sistemas operacionales, sistemas de información, firmas de herramientas antivirus e IDS (*intrusion detection systems*)
	Diagramas de topología de la red y sistemas críticos
	Reportes del desempeño normal de la red, sistemas de información y otros recursos como correo, firewall, sistemas de almacenamiento
Recursos para mitigación de incidentes	
	Medios de almacenamiento
	Parches de seguridad
	Imágenes de respaldo de sistemas operacionales, servidores y sistemas de información.

Anexo B
FORMATO DE DOCUMENTACIÓN DE INCIDENTES

Fecha (dd/mm/aaaa)	Hora (hh:mm)
Nombre de quién diligencia este formulario	
Información de persona de contacto para el incidente	
Nombre	Área/Dependencia
Correo electrónico	Número telefónico
Ubicación física de la persona	

Detalles del incidente						
Fecha y Hora de cuando se descubre del incidente: (dd/mm/aaaa)				Fecha y Horas estimadas de cuando ocurrió el incidente (dd/mm/aaaa)		
Tipo de incidente	Denegación de servicio	Código malicioso	Acceso no autorizado	Uso inapropiado	Multicomponente	No clasificado
Ubicación física del incidente						
Estado actual del incidente						
Descripción del incidente (detalle la fuente/causa si la conoce)						
Detalles de los equipos afectados (redes, servidores, aplicaciones datos)						
Detalles de los sistemas operacionales (tipo, versión, nivel de parches)						
Detalles del antivirus (cuando aplique)						
Impacto estimado del incidente (usar las tablas de cálculo de impacto)						
Acciones de respuesta ejecutadas						
Organizaciones(entidades) que han sido contactadas						
Comentarios generales						

LISTA DE CONTACTOS PARA ATENCIÓN DE INCIDENTES DE SEGURIDAD

Nombre	
Especialidad	
Móvil	
Teléfono fijo	
Email	
PIN Celular (si aplica)	
Mensajería instantánea	
Observaciones	

Nombre	
Especialidad	
Móvil	
Teléfono fijo	
Email	
PIN Celular (si aplica)	
Mensajería instantánea	
Observaciones	

Nombre	
Especialidad	
Móvil	
Teléfono fijo	
Email	
PIN Celular (si aplica)	
Mensajería instantánea	
Observaciones	

Anexo C REGISTRO DE LECCIONES APRENDIDAS RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Fecha	**Moderador**
Lugar	

Participantes

Nombre	Correo electrónico	Firma

Descripción del incidente

Evaluación de la respuesta al incidente

Aspecto	SI/NO
Fue bueno el desempeño del grupo de atención de incidentes	
Fue bueno el desempeño del grupo directivo del INSTITUTO PARA LA ECONOMIA SOCIAL	
Se ejecutaron pasos o acciones que pudieron impedir la recuperación	
Se siguieron los procedimientos documentados	
Fueron adecuados los procedimientos	

Mejoramiento

Qué acciones se deben ejecutar en forma diferente durante la atención de un futuro incidente

Qué herramientas adicionales o recursos son necesarias para detectar, analizar, y mitigar futuros incidentes

Otras observaciones

Anexo D

7 GUÍA PARA LA GESTIÓN DE INCIDENTES DE DENEGACIÓN DE SERVICIOS

7.1 Definición

La denegación de servicios es una acción que previene o imposibilita el uso autorizado de sistemas, servicios, redes o aplicaciones mediante el consumo excesivo de recursos como la CPU, la memoria, el ancho de banda y el espacio en disco. Algunos ejemplos de situaciones que se consideran denegación de servicios (DoS) incluyen pero no se limitan a:

Usar todo el ancho de banda mediante la generación de elevados volúmenes de tráfico. Esta situación se puede presentar cuando se descargan videos, música o se emplea la red para comunicaciones de voz o video en sistemas como Skype, Messenger u otros programas de mensajería instantánea.

Envío de paquetes TCP/IP mal formados hacia un servidor provocando que el sistema operacional falle

- Envió de solicitudes ilegales a una aplicación para provocar que falle
- Realizar múltiples solicitudes intensas al procesador de un computador de forma que todo el recurso de procesamiento del equipo se agote.
- Establecer múltiples conexiones de autenticación a una aplicación para impedir que nuevos usuarios puedan ingresar al sistema.
- Realizar difusión masiva de paquetes en la misma frecuencia empleada por una red inalámbrica para hacer inservible el servicio de red.
- Consumir todo el espacio en disco mediante la creación de archivos masivos o archivos de gran tamaño.

Los ataques de DoS se han vuelto cada vez más frecuentes y son una amenaza de alta probabilidad de ocurrencia en páginas web, servicios de correo u otros sistemas de información causando perturbación en la prestación del servicio. En sentido estricto ninguna organización se pueden proteger al 100% de un ataque de DoS, en este documento se exponen algunas medidas preventivas que deben ser evaluadas por el [oficial o encargado de seguridad de la información].

NOTA: a continuación se describe un resumen muy general de los componentes

de un ataque de Denegación de Servicio, se invita al lector a consultar literatura especializada al respecto para comprender la naturaleza de este tipo de ataques.

Un ataque de DoS emplea dos tipos de componentes que trabajan en conjunto para comprometer al servidor bajo ataque. El primero son los agentes que corren en los servidores y que son los que en realidad ejecutan el ataque y un controlador que es un programa que administra a los agentes para darles las ordenes de ataque (qué, cuándo y cómo). Los agentes reciben regularmente el nombre de *bots*, el conjunto de servidores afectados se denominan *botnet.* En algunas ocasiones el atacante no usa un controlador (hadler) para controlar el botnet y puede hacer uso de canales de comunicación como IRC. Otras formas de ataque incluyen la pre-programación de los bots para que actúen bajo unas condiciones predeterminadas. Los ataques por lo general involucran un número elevado de botnets para lograr el volumen de requerimientos de servicios para provocar la denegación de servicios.

Se han identificados tres tipos de ataque DoS, a continuación se describen en forma general las características de los tipos de ataque.

Ataque *Reflector* (espejo)
En un ataque Reflector un servidor envía múltiples solicitudes con una dirección IP falsificada un servicio en un servidor intermedio. (Por lo regular se usan servicios basados en protocolo UDP). El servidor responde a la petición empleando la dirección falsificada, de esta forma el servidor que responde es quien aparece como ejecutante del ataque y por esa razón se denomina el reflector (espejo). El ataque de DOS puede tener como objetivo el servidor cuya dirección fue falsificad o el servidor que actúa como el reflector. Los puertos que por lo general son empleados por el ataque son: echo (puerto 7), chargen (puerto 9), DNS (puerto 53), SNMP (puerto 161) e ISAKMP (puerto 500). En el ataque también se pueden emplear dos reflector, el atacante envía la petición al primer servidor obligándolo a enviar una segunda petición con dirección falsa a un tercer servidor que actuaría como el reflector generador del ataque, en algunas ocasiones se puede generar un loop de peticiones entre los dos reflectores.

La mayoría de los ataques de reflector se pueden prevenir con un firewall configurado en modo network-based o host-base para que pueda rechazar combinaciones sospechosas de puertos origen y destino.

Ataque amplificados
Al igual que un ataque por reflector, se emplea una petición con una dirección IP falsa un servidor intermediario. A diferencia del ataque por un reflector, el objetivo será emplear toda una red como elemento intermediario para el ataque. La

intención es emplear una petición ICMP o UDP a una dirección de Broadcast para que muchos servidores respondan a la misma, como la dirección es falsa toda la red responderá al servidor que será víctima del ataque.

Muchos de los ataques amplificados se pueden bloquear configurando routers de borde para que no reenvíen tráfico broadcast a menos que esté autorizado.

Otra forma de ataque amplificado es el denominado DNS recursivo. En esta forma de ataque si un DNS está configurado para permitir recursividad procesara solicitudes de dominios para los cuales no es un DNS autoritativo. Durante un ataque de DNS recursivo el atacante envía miles de solicitudes con dirección falsa a un DNS que permite recursividad. Estas solicitudes son procesadas por el DNS y respondidas al dueño de la dirección falsa (la de la víctima). En este tipo de ataque gigabytes de respuestas DNS son reflejadas a la dirección falsa lo que causa su saturación.

Ataques Flood (inundación)
En un ataque por inundación, un servicio o recurso se hace indisponible iniciando una elevada serie de solicitudes de conexión incompletas. Este tipo de ataque satura al receptor imposibilitándolo para atender nuevas conexiones. Algunas de las formas de realizar el ataque incluyen:

Peer-to-peer attack:
Desconectar un archivo compartido por protocolo peer-to-peer y redirigir todas las solicitudes del archivo compartido a la dirección de la víctima, de esa forma miles de equipos que buscan el archivo compartido redirigen sus peticiones al sitio web de la víctima.

Synflood:
En este tipo de ataque el atacante genera múltiples solicitudes de conexión con la trama SYN pero no completa los tres pasos de la conexión con lo cual si el sistema operacional no está preparado para cancelar las solicitudes de conexión incompletas, agotara todos sus recursos dejando pendiente múltiples solicitudes de conexión abiertas.

7.2 Preparación para responder a un ataque de DOS

A continuación se describen algunas estrategias que se pueden usar para manejar ataques por denegación de servicio.

Preparación previa para el manejo del incidente:

- Coordinar con el ISP mecanismos para prevenir ataques de denegación de

servicio network-based. Algunas estrategias incluyen: filtrado de tráfico, mantener log de direcciones de donde se han generado ataques de DOS y rechazar el tráfico de esas fuentes. Establecimiento claro de procedimientos con el ISP cuando se requiere soporte de primer o segundo nivel, definición de los puntos de contacto en caso de emergencia, mantenimiento de múltiples canales de comunicación para reportar incidentes y métodos que debe emplear el ISP para verificar la autenticidad de las solicitudes.

- Instalar y configurar un sistema de detección de intrusos para identificar ataques por denegación de servicios

- Instalar y configurar un sistema de supervisión de consumo de recursos como el ancho de banda para establecer la línea base de consumo del recurso y generar alertas cuando se sobrepasen los umbrales establecidos.

- Identificar los sitios web que pueden suministrar servicios de *Internet health monitoring*, por ejemplo *http://www.internetpulse.net/.,* para identificar latencia en los servicios de DNS y así establecer si el ataque de DOS es un ataque masivo que afecta a muchas organizaciones.

- Definir protocolos de respuesta con los administradores de red para que ajusten los umbrales de registro de eventos de red durante el ataque para mantener las evidencias.

- Mantener segura y actualizada la configuración de equipos de red (papel y electrónica) que son indispensables para atender el ataque y para reconstruir la configuración de la red en caso de afectación grave.

7.3 Prevención del incidente

Las siguientes recomendaciones son medidas preventivas: Configuración de un perímetro seguro de red para rechazar toda solicitud que no provenga de perímetros seguros de red. Esta acción incluye: bloqueo de tráfico innecesario, filtrar puertos y direcciones que no correspondan al perímetro seguro o a direcciones no asignadas, configurar los switchs de borde para que no reenvíen peticiones de broadcast. Limitar el tráfico ICMP. Bloquear conexiones salientes a servicios IRC, peer-to-peer y puertos de mensajería instantánea si no son necesarios para el desarrollo del trabajo de los empleados y funcionarios. Limitar el nivel de consumo de protocolos como ICMP para que solo puedan usar un porcentaje definido del ancho de banda disponible. En todo servidor visible desde internet deshabilitar todo puerto o servicio que no sea necesario. Implementar redundancia en servicios clave: ISP, firewall, Servidores página Web, Correo.

Verificar que los servicios y servidores no estén operando a niveles cercanos a su capacidad máxima para evitar que un ataque DOS los colapse rápidamente.

7.4 Análisis y detección

Los ataques DoS se pueden identificar mediante una serie de precursores e indicadores algunos de los cuales se muestran en las siguientes tablas.

Precursores de ataques de denegación de servicios	
Precursor	**Respuesta**
Por lo general la DoS está precedida por una actividad de reconocimiento, por lo regular un volumen bajo de tráfico que se usa para verificar si el ataque será efectivo	Si los respondientes detectan actividad inusual que parece ser la preparación para un ataque de DoS, se debe evaluar la posibilidad de bloquear el ataque a la mayor brevedad posible ajustando reglas del firewall para bloquear los protocolos que puedan ser usados para el ataque
Una nueva herramienta de DoS puede indicar una amenaza significativa para la entidad	Si es posible, se debe indagar sobre la nueva herramienta y ajustar los controles de seguridad del firewall de forma que la herramienta no sea efectiva para realizar el ataque.

Indicadores de denegación de servicio	
Acción maliciosa	**Posibles indicadores**
DoS Network-based contra un servidor en particular	El usuario reporta no disponibilidad de un sistema Perdida inexplicable de conexión El IDS genera alerta intrusión Aumento en la utilización de ancho de banda Número elevado de conexiones hacia un servidor Patrones asimétricos de tráfico en la red (elevado volumen de tráfico saliendo del servidor pero muy poco trafico entrante) Registros anómalos en el firewall o router Paquetes con direcciones fuente inusuales
Network-based DoS en contra de una red	El usuario reporta no disponibilidad de un sistema Perdida inexplicable de conexión El IDS genera alerta intrusión Aumento en la utilización de ancho de banda Número elevado de conexiones hacia un servidor Patrones asimétricos de tráfico en la red (elevado

Indicadores de denegación de servicio	
Acción maliciosa	**Posibles indicadores**
	volumen de tráfico saliendo del servidor pero muy poco trafico entrante) Registros anómalos en el firewall o router Paquetes con direcciones fuente inusuales Paquetes con direcciones de destino inexistentes
DoS contra el sistema operacional de un servidor específico	El usuario reporta no disponibilidad de sistema o un aplicación El IDS genera alerta intrusión Registros de alerta en el sistema operacional Paquetes con direcciones fuente inusuales
DoS en contra de la aplicación en un servidor en particular	El usuario reporta no disponibilidad de sistema o un aplicación El IDS genera alerta intrusión Registros de alerta en la aplicación Paquetes con direcciones fuente inusuales

7.5 Contención, erradicación y recuperación

A continuación se relacionan algunas recomendaciones sobre la estrategia de manejo de un ataque DoS.

7.5.1 Selección de la estrategia de contención

La contención de un incidente de DoS por lo general consistirá en detener el ataque. Debido a que la dirección fuente original del ataque no se puede obtener con facilidad porque el atacante usa una dirección falsa, tratar de bloquear la dirección fuente del ataque no siempre es factible, aún si se logra identificar, el atacante se puede mover a otra dirección. Otras posibles soluciones incluyen:

- Corregir la vulnerabilidad o debilidad que está siendo explotada. Por ejemplo, habilitar el bloqueo del puerto que se está usando para el ataque, cerrar los servicios que están siendo explotados para el ataque, como por ejemplo el “echo”. Parchar los sistemas operacionales con versiones actualizadas que corrijan las vulnerabilidades, para ese fin el servidor debe ser desconectado temporalmente de la red mientras se rectifica la vulnerabilidad.

- Implementar el filtrado de paquetes basado en el patrón de comportamiento del ataque. Si por ejemplo el ataque se basa en tráfico ICMP, se debe implementar el filtrado de red de ese tipo tráfico, se debe tener cuidado con esta opción porque si el tráfico que usa el atacante es SYN hacia un servidor WEB, la medida de contención generará un DOS hacia el servidor

WEB. Otra opción es limitar el volumen de tráfico del protocolo que esté usando el atacante, esta medida también puede ser contraproducente porque el desempeño de los servicios se puede ver afectado si se limita el tráfico, se debe evaluar cuidadosamente si se aplica el filtrado de tráfico en caso de que el ataque se prologue por días o más tiempo.

- Solicitar al ISP que filtre el tráfico Cuando el ataque se origina desde una red externa, el volumen de tráfico generado sobrecargara la red y será necesario el apoyo del ISP para filtrar el tráfico generado por la red externa.

- Relocalizar el objetivo: Si un servidor está bajo ataque y las estrategias anteriores no han sido efectivas el servidor puede ser movido a otra dirección IP, no siempre funcionara porque el atacante puede redirigir su ataque a la nueva dirección. De igual forma el puerto del servicio bajo ataque se puede mover a otro servidor que no tenga la misma vulnerabilidad.

- Atacar al atacante: Un opción puede ser utilizar programas para bajar en forma remota los agentes instalados en el servidor que está generando el ataque o reconfigurar los servidores bajo ataque para que reboten el tráfico hacia el atacante, esta técnica puede afectar a un servidor inocente si su dirección fue hurtada. Esta técnica debe ser usada con mucho cuidado.

7.5.2 Recolección de evidencias del ataque

La recolección de las evidencias de un ataque de DoS pueden ser complejas debido a:

- Identificar la fuente del ataque a partir del tráfico observado: Por lo regular la dirección es falsa.
- Identificar la fuente del ataque con la ayuda del ISP: Si es viable el ISP puede apoyar en la identificación del origen del ataque, pero debido a la cantidad de tiempo que esta tarea puede consumir, el ataque puede haber terminado antes de lograr identificar la fuente del mismo.
- Revisión de los registros: Debido a la naturaleza del ataque se generan elevados volúmenes de registros que quedan almacenados en los firewall, IDS y sistemas operacionales.

Lista de chequeo de acción para manejo de ataques de denegación de servicio	
Acción	**Completa?**
Análisis	
1. Priorizar el manejo del incidente de acuerdo con el impacto a la misión de la entidad	
1.1 Identificar los recursos han sido afectados y proyectar que recursos podrían ser afectados	
1.2 Estimar los efectos técnicos reales y potenciales del incidente	
1.3 Identificar el nivel correcto de priorización del incidente de acuerdo con las matrices de evaluación de impacto	
2 Notificar el incidente a las instancias apropiadas	
Contención, erradicación y recuperación	
3 Adquirir, preservar, asegurar y documentar la evidencia	
4 Contener el incidente si no ha sido contenido aún	
4.1 Identificar y mitigar vulnerabilidades	
4.2 Si no está contenido implementar filtrado de paquetes basado en las características del ataque	
4.3 Si no está contenido contactar al ISP para solicitar su apoyo	
4.4 Si no está contenido relocalizar el objetivo	
5 Erradicar el incidente. Si no se han eliminado las vulnerabilidades, identificar y mitigar las mismas	
6 Recuperación del incidente	
6.1 Retornar los sistemas y servicios afectados a su estado normal	
6.2 Confirmar que los sistemas afectados funcionan correctamente	
6.3Si es necesario y factible implementar acciones complementarias de supervisión para identificar nuevas situaciones	
Revisión post incidente	
7 Crear un reporte de seguimiento	
8 Realizar una sesión de lecciones aprendidas.	

7.6 Resumen de recomendaciones para el manejo de ataques de denegación de servicios

- Configurar el firewall para prevenir ataques en espejo (reflector)
- Configurar los *routers* de borde para prevenir ataques amplificados
- Determinar los mecanismos de soporte del ISP para atender requerimientos de primer y segundo nivel para ataques de denegación de servicio
- Configurar el software de seguridad (IDS) para detectar ataques de denegación de servicios

- Configurar el perímetro de red para negar todo tráfico entrante o saliente que no esté expresamente autorizado
- Crear una estrategia de contención que incluya una secuencia de soluciones

Anexo E

8 GUÍA PARA LA GESTIÓN DE INCIDENTES DE CÓDIGO MALICIOSO

8.1 Definiciones

De acuerdo con las definiciones de la norma NIST 800-61, Un código malicioso se refiere a un programa que es insertado en otro programa con la intención de destruir datos, ejecutar programas destructivos o instructivos u otras acciones que comprometen la confidencialidad, integridad y disponibilidad de los datos de la víctima. Esta fuera de esta guía realizar una descripción detallada de las diferentes categorías de código malicioso, se invita al lector a consultar las normas NIST 800-61, NIST 800-83 y otros tipos de fuentes para ampliar los conceptos relacionados con la definiciones de código malicioso, por ejemplo http://www.sophos.com/security/ o http://www.trendmicro.com/vinfo/virusencyclo.

Dentro de las posibles variaciones de código malicioso se deben considerar pero no limitarse a: Virus, gusanos, Troyanos, código móvil, backdoors, rootkits, keyloggers, tracking cookies, spyware

Virus: Software diseñado para auto replicarse y distribuir copias de sí mismo para infectar a archivos o sistemas. Los virus se puede catalogar de acuerdo con su modelo de ataque en: File Infector Virus, Boot Sector Virus, Multipartite Virus. Otra forma de catalogarlos es por el tipo de construcción como: compilados e interpretados. Dentro de los interpretados se debe prestar especial atención a los que se construyen empleado lenguajes de programación habilitados para documentos como procesadores de texto. En esta última categoría pueden encontrarse: Macro Virus y Scripting Virus.

Gusanos: es software auto-replicante que está completamente contenido en sí mismo, lo que significa que no necesita de otro programa para propagarse hacia sus víctimas. Los gusanos se pueden clasificar como: *Network Service Worms y Mass Mailing Worms*.

Cabayos Troyanos (*Trojan Horses*): Son programas que no tienen capacidad de auto-replicarse y que pretenden estar realizando acciones benéficas mientras que en realidad están efectuando acciones nocivas.

Código malicioso móvil: es software que se transmite desde un sistema remoto hacia la victima sin que se requiera instrucción expresa del usuario. Los lenguajes más populares para escribir código malicioso móvil incluyen: Java, ActiveX, JavaScript, y VBScript.

Código malicioso combinado: es el software que emplea varios mecanismos de ataque (correo, servidores web, clientes vía web, etc.)

Tracking Cookies: pieza particular de software que recopila información acerca del uso particular de un sitio web.

Backdoor: en líneas generales es un código que escucha comandos sobre ciertos puertos que corran protocolos como TCP o UDP para ejecutar acciones como: transferir archivos, extraer passwords o ejecutar comandos.

Keylogger: es software que tiene como objetivo supervisar y grabar el uso del teclado en el computador en donde se instala el software malicioso, el software puede grabar contenido de claves, correos electrónicos, nombres de usuarios, números PIN.

Rootkit: es una colección de software que se instala en el sistema para modificar su comportamiento de manera maliciosa, los rootkit alteran varios archivos de los sistemas operacionales y modifican archivos ejecutables para lograr que se oculte la existencia del rootkit.

Web browser plug-in: algunos plugin para los navegadores web pueden ser desarrollados como software malicioso para que actúen como spyware.

Además de las anteriores categorías existen dos amenazas que con frecuencia se catalogan como código de malicioso, pero no lo son. Estas dos variantes son: phishing y hoax. Estas dos amenazas emplean técnicas de ingeniería social para intentar que sus víctimas revelen información confidencial o descarguen software que si es código malicioso.

8.2 Preparación

Está sección proporciona directrices para la atención de incidentes clasificados como ataques de código malicioso.

8.2.1 Preparación para el manejo del incidente

Las siguientes son directrices complementarias a las indicaciones del procedimiento general de respuesta a incidentes de seguridad de la información.

- Sensibilizar a los usuarios sobre los problemas del código malicioso: se deben realizar charlas periódicas sobre el comportamiento de código malicioso, métodos de ataque, medidas de prevención.

- Revisar los boletines de los vendedores de software de control de código malicioso: Los miembros del grupo de respuesta a incidentes; visitar periódicamente (al menos 1 vez por semana) los sitios web de proveedores de soluciones reconocidas de control de código malicioso para conocer nuevas amenazas.

- Configurar los sistemas de detección de intrusos para supervisar servidores críticos: El software de IDS puede supervisar síntomas de código malicioso tales como cambios en archivos ejecutables o archivos de configuración

- Recolectar información para el análisis de código malicioso: El grupo de respuesta a incidentes debe mantener actualizada una librería de información relacionada con el comportamiento de código malicioso, la información puede estar en sitios web de fabricantes, grupos de interés especializados o bases de datos gestionadas directamente por el grupo de respuesta a incidentes.

- Adquirir software de mitigación de código malicioso: las herramientas que se deben mantener actualizadas para atender este tipo de incidentes incluyen: software de antivirus, copia de medios de sistemas operacionales originales, discos de arranque limpios, parches de seguridad, backups limpios de los datos.

8.2.2 Prevención del incidente

Las siguientes acciones complementan las recomendaciones del procedimiento general de atención a incidentes. Se deben ejecutar las acciones del procedimiento general y las recomendaciones específicas para la atención de incidentes de código malicioso.

- Uso de software de antivirus: El software de antivirus es esencial para gestionar los incidentes de código malicioso. El software de antivirus debe estar instalado, actualizado y ejecutándose en todas las estaciones de trabajo del INSTITUTO PARA LA ECONOMIA SOCIAL. Además de las estaciones de trabajo los servidores de correo electrónico deben tener configurado su software de control de virus y spam. De igual forma sobre los servidores dedicados a filesystem compartido se deben realizar pruebas periódicas de detección de código malicioso con el software de antivirus. El software de antivirus de las estaciones de trabajo debe estar configurado para verificar todo archivo que se abra, descargue o utilice en las estaciones de trabajo y debe estar habilitada la inspección a intervalos definidos por el [oficial o encargado de seguridad de la información] de los filesystem de servidores y estaciones de trabajo.

- Prevención de instalación de software spyware: Los navegadores web deben ser configurados para que no se permita la instalación de plugins o software no autorizado. Se debe instalar software de control de spyware en las estaciones de trabajo, si el software de antivirus de la estación de trabajo cuenta con módulos de antispyware estos deben estar actualizados y habilitados para impedir la instalación de este tipo de código malicioso.

- Bloquear archivos sospechosos: Los servidores de correo electrónico y clientes de correo electrónico se deben configurar para que bloqueen archivos con extensiones asociadas a fuentes conocidas de código malicioso (vbs. pif, exe pps), y combinaciones sospechosas de extensiones (.txt.vbs,.html.exe)

- Filtrado de spam: se deben configurar los servidores de correo electrónico y clientes de correo para que filtren los correos clasificados como spam, los servicios de filtrado de spam deben estar instalados, configurados y permanentemente actualizados.

- Limitar el uso de programas de transferencia de archivos que no son necesarios para el cumplimiento de funciones de la entidad: todo programa cuyo de transferencia de archivos que no sea autorizado para una función misional debe ser deshabilitado y desinstalado, esto incluye programas para compartir música, video, programas que empleen protocolos como ftp, chat, videoconferencia o audioconferencia.

- Educar a los usuarios sobre la forma segura de usar archivos adjuntos: Los servicios de antivirus deben ser configurados para que se verifique cualquier archivo antes de que se pueda abrir, eso incluye archivos pps, ppt, doc, xls, etc. Los usuarios deben ser alertados de no abrir archivos adjuntos que no procedan de fuentes seguras o autorizadas, el usuario debe ser alertado acerca de que a pesar de que el remitente sea conocido los archivos adjuntos pueden estar contaminados, se debe instruir a los usuarios para que no abran adjuntos con extensiones como.exe,.vbs,.pps,.bat,.com,.pif.

- Supervisar los contenidos de los directorios compartidos: los directorios compartidos del sistema operacional Windows facilitan la propagación de código malicioso hacia los equipos que comparten o usan los directorios, el uso de dichos directorios debe estar debidamente autorizado, supervisado y verificado su contenido regularmente.

- Limitar el uso de código móvil en los navegadores: el uso o habilitación de código móvil (active x, java, plugins javascript) debe ser autorizado por el [oficial o encargado de seguridad de la información], la autorización se debe realizar previa verificación de los sitios web que así lo requieran. El firewall debe ser configurado para filtrar tráfico de código móvil no autorizado.

- Configurar el servidor de correo electrónico para prevenir *OPEN RELAY:* el servidor de correo electrónico debe ser configurado para evitar que sea usado como Open Relay, el servidor solo debe permitir la generación de correos electrónicos desde el dominio del INSTITUTO PARA LA ECONOMIA SOCIAL.

- Configurar en forma segura los clientes de correo: los clientes de correo electrónico deben ser configurados para impedir apertura automática de archivos, ejecución de archivos no autorizados.

8.3 Detección y Análisis de los incidentes

Los incidentes de código malicioso deben ser identificados rápidamente debido a que su velocidad de propagación es muy alta y puede infectar a muchas estaciones de trabajo en pocos minutos.

En la siguiente tabla se describen algunos de los precursores que se pueden emplear para detectar los incidentes de código malicioso.

Posibles precursores de incidentes de código malicioso	
Precursor	**Respuesta**
Una alerta advierte sobre nuevas formas de código malicioso que ataca al software que utiliza la entidad	Se debe realizar investigación sobre el nuevo tipo de código malicioso. La investigación se puede realizar con información de los proveedores de software de control. Verificar la autenticidad de la alerta y de ser cierta verificar la actualización de las herramientas de control de código malicioso (antivirus, antispyware, etc.). Si no están disponibles las nuevas firmas del código malicioso se deben emplear mecanismos como bloquear mensajes de correo, restringir el uso de puertos o cerrar servicios vulnerables.
El antivirus detecta, desinfecta de manera exitosa o coloca en	Determinar cómo ingresó el código malicioso a la red que vulnerabilidad o debilidad se

cuarentena archivos sospechosos o infectados	intentaba explotar. Si la exposición al riesgo es muy elevada se debe mitigar la vulnerabilidad lo antes posible.

Indicadores de incidentes de código malicioso	
Acción maliciosa	**Posible indicador**
Un virus que se dispersa por correo electrónico infecta un servidor	• El software de antivirus alerta de archivos infectados • Sin razón aparente crece el número de correos electrónicos entrantes o salientes • Se presentan cambios en las plantillas de creación de documentos, hojas electrónicas, etc. • Archivos borrados, alterados o dañados sin razón aparente • Elementos inusuales en la pantalla como mensajes extraños o gráficas no definidas • El sistema se hace inestable o se cae • Si el virus captura la cuenta del superusuario se debe verificar la lista de comprobación de la guía de respuesta a incidentes de acceso no autorizado.
Un gusano que se propaga a través de un servicio vulnerable infecta un servidor.	• El Antivirus alerta sobre archivos infectados • Se detecta exploración “scaneo” de puertos y conexiones fallidas cuyo objetivo es el servicio afectado • Incremento injustificado del uso de la red • Los programas inician en forma lenta, presentan lentitud durante la ejecución o no se ejecutan • El sistema se comporta inestable o se cae • Si el gusano captura la cuenta del superusuario se debe verificar la lista de comprobación de la guía de respuesta a incidentes de acceso no autorizado
Un caballo troyano se instala y se ejecuta en un servidor	• El software de antivirus detecta versiones de caballos troyanos • El IDS detecta o alerta sobre caballo troyano en las comunicaciones cliente.-servidor • Los registros del firewall o el router muestran presencia de software tipo caballo de troya • Se presentan conexiones desconocidas entre el servidor y un sistema remoto desconocido • Procesos desconocidos en ejecución • Aumento injustificado de tráfico en la red generado

Indicadores de incidentes de código malicioso	
Acción maliciosa	**Posible indicador**
	desde un servidor en particular dirigido a un sistema externo. • Los programas inician en forma lenta, presentan lentitud durante la ejecución o no se ejecutan • El sistema se comporta inestable o se cae • Si el caballo de Troya captura la cuenta del superusuario se debe verificar la lista de comprobación de la guía de respuesta a incidentes de acceso no autorizado
Un código móvil malicioso en un servidor web se usa para infectar un servidor con un virus, un gusano o un caballo de Troya	• Se presentan los indicadores de virus, gusano o caballo de Troya • Se abren ventanas de dialogo solicitando permiso para acciones desconocidas o conocidas pero no solicitadas • Gráficos inusuales como sobre posición de pantallas o mensajes sobre escritos.
Código malicioso en un servidor web explota una vulnerabilidad en un servidor	• Se abren ventanas de dialogo solicitando permiso para acciones desconocidas o conocidas pero no solicitadas • Gráficos inusuales como sobre posición de pantallas o mensajes sobre escritos. • Sin razón aparente crece el número de correos electrónicos entrantes o salientes • Sin razón aparente crece el número de correos electrónicos entrantes o salientes • Si el código malicioso captura la cuenta del superusuario se debe verificar la lista de comprobación de la guía de respuesta a incidentes de acceso no autorizado
El usuario recibe un mensaje de virus hoax	La fuente original del mensaje no es un organismo autorizado para emitir la alerta No existen enlaces a fuentes externas El tono y terminología del correo induce al pánico o elevado sentido de urgencia Se solicita urgentemente al usuario realizar acciones como borrar archivos y reenviar correos a otros usuarios

El proceso de identificación de los ataques por código malicioso puede ser

complejo debido a que otras causas pueden generar caída de un servidor web o comportamiento lento de un programa. Es vital que el grupo de atención de incidentes de seguridad se entrene en la identificación del malware, la priorización de este tipo de incidentes es relativamente simple, debido a que su velocidad de propagación es elevada y puede afectar rápidamente a muchas estaciones de trabajo.

El grupo de respuesta a incidentes debe considerar los siguientes aspectos cuando determine la estrategia de tratamiento de incidente:

- Cómo ingreso el código malicioso a la infraestructura del INSTITUTO PARA LA ECONOMIA SOCIAL
- Qué mecanismos de transmisión usa
- Qué tipo de malware es (virus, troyano, spam)
- Qué tipo de herramientas de ataque la instalado el código malicioso
- Qué infraestructura y sistemas han sido afectados
- Que comportamiento tendrá el ataque en los próximos minutos, horas y días en caso de que el incidente no se contenga correctamente

8.4 Contención, Erradicación y Recuperación

Además de las acciones genéricas del procedimiento de respuesta a incidentes, se deben ejecutar las acciones particulares que se describen a continuación.

8.4.1 Selección de estrategia de contención

Los incidentes de código malicioso se deben contener rápidamente debido a su alta velocidad de propagación. Si el sistema afectado no es crítico para las funciones del INSTITUTO PARA LA ECONOMIA SOCIAL se debe proceder a su desconexión de la red, si el sistema es de naturaleza crítica se debe evaluar si el impacto de desconectarlo es mayor que el daño que genera el código malicioso.

Además de las anteriores consideraciones se debe verificar la aplicación de las siguientes acciones

- Aplicar las acciones de prevención de incidentes de código malicioso descritas anteriormente
- Identificar y aislar los sistemas afectados
- Remitir el código malicioso detectado al proveedor del software de antivirus del INSTITUTO PARA LA ECONOMIA SOCIAL
- Configurar el servidor de correo y los clientes para bloquear los email que transportan el código malicioso
- Bloquear los servidores que fueron infectados impidiendo que se conecten

a servidores externos o internos
- Bajar el servidor de correo
- Aislar la red del INSTITUTO PARA LA ECONOMIA SOCIAL de la conexión a internet
- Informar a los usuarios de las acciones que debe seguir para evitar la propagación del código malicioso
- Deshabilitar los servicios que han sido comprometidos en el incidente
- Deshabilitar el acceso a redes que están comprometidas o que por su criticidad deben ser protegidas del ataque.

8.4.2 Recolección y mantenimiento de evidencias

Aunque la recolección de evidencias de un incidente puede ser relativamente simple, puede ser una acción inútil debido que el código malicioso se propaga sin intervención de atacantes y la recolección de estas evidencias no sería útil para iniciar procesos legales. Existen tres posibles técnicas para recolectar evidencias:

Identificación forense: consiste en el uso de evidencias generadas por recientes ataques para identificar la causa y fuente del ataque

Identificación activa: consiste en el uso de técnicas para identificar los sistemas que están infectados.

Identificación manual: Es la tarea que más tiempo y esfuerzo consume debido a que consiste en que los mismos usuarios o el personal de tecnología por si mismos identifique los síntomas, extensión. En esos casos se debe tener entrenamiento especializado o un grupo técnico capacitado para realizar la tarea.

8.4.3 Erradicación y recuperación

Se debe usar software de antivirus y antispyware actualizado y efectivo para eliminar el código malicioso. En caso de que el software no erradique el virus, se debe evaluar la posibilidad de borrar los archivos infectados y reemplazarlos con copias limpias de los mismos. En algunos casos puede ser necesario reinstalar el software contaminado. Si el código ha capturado el acceso del superusuario se recomienda proceder con una reinstalación completa y limpia del sistema debido a que no es fácil determinar que modificaciones se efectuaron al sistema con la clave del superusuario. Si se debe reinstalar el sistema se debe proceder inmediatamente a su aseguramiento o endurecimiento (*hardenning*) para prevenir futuros incidentes.

Lista de chequeo para atención de incidentes de código malicioso		
Paso	**Acción**	**Completada?**
Análisis		
1	Priorizar el manejo del incidente de acuerdo con el impacto para la función misional del INSTITUTO PARA LA ECONOMIA SOCIAL	
1.1	Identificar que recursos han sido afectados y estimar que recursos podrían ser afectos	
1.2	Estimar el impacto real y potencia del incidente	
1.3	Identificar en la matriz de impacto el nivel de prioridad del incidente	
2	Reportar el incidente a la instancias pertinentes	
Contención y erradicación		
3	Contener el incidente	
3.1	Identificar los sistemas afectados	
3.2	Desconectar los sistemas afectados de la red	
3.3	Mitigar las vulnerabilidades que han sido usadas por el código	
3.4	Si es necesario bloquear las comunicaciones del sistema afectado para impedir la propagación del código	
4	Erradicar el incidente	
4.1	Desinfectar, poner en cuarentena, borrar o reemplazar, según sea el caso los archivos afectados	
4.2	Mitigar las vulnerabilidades explotadas en los demás servidores o estaciones de trabajo	
5	Recuperarse del incidente	
5.1	Confirmar que los sistemas afectados funcionan normalmente	
5.2	Si es necesario implementar mecanismos adicionales de supervisión para identificar actividades futuras de ataque	
Revisión post incidente		
6	Crear reporte de seguimiento del incidente	
7	Realizar reunión de lecciones aprendidas	

Anexo F

9 GUÍA PARA LA GESTIÓN DE INCIDENTES DE ACCESO NO AUTORIZADO

9.1 Definiciones

Un incidente de acceso no autorizado ocurre cuando una persona obtiene acceso a un recurso para el cual no está autorizado. El acceso no autorizado se logra cuando se explota una vulnerabilidad del sistema operacional o de una aplicación, cuando se obtienen usuarios o claves o mediante ataques de ingeniería social. Los atacantes usualmente obtienen acceso limitado a partir de la vulnerabilidad y mediante ese acceso buscan elevar su nivel de privilegios de acceso.

Algunos ejemplos de acceso no autorizado incluyen:

- Comprometer la cuenta del superusuario de un servidor de correo
- Capturar un servidor de páginas web
- Adivinar o romper password
- Ver o copiar información sensible sin tener autorización como registros de nómina, información de hoja de vida médica, números de tarjetas de crédito
- Ejecutar programas para exploración o indagación de redes como sniffer o scanners, para observar nombres de usuario o claves
- Usar un filesystem compartido para distribuir software ilegal o copias ilegales de software
- Suplantar una persona ante la mesa de ayuda para solicitar el cambio de claves
- Usar un computador desatendido sin la debida autorización

9.2 Preparación

Las siguientes recomendaciones sobre la atención de incidentes de acceso no autorizado complementan las recomendaciones generales del procedimiento de respuesta a incidentes. El grupo de respuesta a incidentes debe ejecutar las recomendaciones generales y las recomendaciones específicas.

9.2.1 Preparación para gestión del incidente

Además de las actividades de preparación genéricas del manual de respuesta a incidentes, se deben ejecutar las siguientes acciones particulares:

- Configurar software de detección y prevención de intrusos.
- Instalar software de verificación de integridad en los servidores
- Efectuar cambios obligatorios de las claves de usuario cuando el password de una aplicación, servidor o sistema ha sido comprometido

por divulgación no autorizada.

- Verificar con los administradores de los sistemas los incidentes de seguridad para ellos comprendan sus roles y responsabilidades en la gestión de incidentes

9.3 Prevención de los incidentes

Los responsables de tecnología del INSTITUTO PARA LA ECONOMIA SOCIAL deben aplicar las recomendaciones de prevención de incidentes que se exponen en el procedimiento de manejo a incidentes. Si se aplican las recomendaciones, el número de incidentes de acceso no autorizado se reducen significativamente.

Acciones para prevenir incidentes de acceso no autorizado	
Categoría	**Acciones específicas**
Seguridad de red	• Configurar perímetros de red para rechazar el ingreso de tráfico que no esté expresamente autorizado. • Asegurar apropiadamente todos los accesos remotos incluyendo VPN • Configurar los servicios públicos en segmentos de zona desmilitarizada (DMZ) • Usar direcciones IP privadas para los servidores en las redes internas
Seguridad de servidores	• Realizar análisis de vulnerabilidades, pruebas de penetración y auditorias de seguridad a los servidores periódicamente • Deshabilitar todo servicio que no sea indispensable para los servidores • Separar los servicios críticos para que se ejecuten en servidores independientes • Ejecutar los servicios con el mínimo número de privilegios necesarios • Instalar, configurar y mantener firewalls para protección de los segmentos de red. • Limitar el acceso físico a servidores • Configurar las cuentas de usuario para que se cierren después de un período de inactividad prolongado. • Verificar en forma periódica los permisos de archivos críticos de configuración de servicios (claves, archivos de configuración)

Acciones para prevenir incidentes de acceso no autorizado	
Categoría	**Acciones específicas**
Autenticación y autorización	• Hacer cumplir la política de claves seguras • Emplear mecanismos de doble autenticación (clave y sistema biométrico) para tener acceso a los servicios, servidores y recursos considerados críticos • Seguir los procedimientos para asignación, cambio y retiro de cuentas de usuario
Seguridad física	• Se debe restringir el acceso físico a servidores y centros de cómputo solamente a personal autorizado.

9.4 Detección y análisis

La siguiente es una lista simplificada de los precursores que pueden indicar un incidente de acceso no autorizado.

Posibles precursores de incidentes de acceso no autorizado	
Acción	**Respuesta**
Los incidentes de acceso no autorizado están precedidos por actividades de reconocimiento de servidores e identificación de vulnerabilidades. Las actividades incluyen exploración de puertos, exploración de servidores, exploración de vulnerabilidades, comandos ping, comandos *traceroute*, transferencias de zonas DNS, identificación de huella de sistema operacional. Las anteriores actividades pueden ser detectadas por un IDS/IPS y análisis de registros.	Se deben buscar cambios en el comportamiento de los servicios y servidores. Si se detecta una vulnerabilidad en la actividad que se está explorando se debe proceder a resolverla para evitar el ataque
Se pública una nueva forma de explotar una vulnerabilidad y expone al INSTITUTO PARA LA ECONOMIA SOCIAL a una amenaza significativa	Se debe investigar sobre la vulnerabilidad y en caso de que sea factible proceder a ajustar los controles de seguridad para reducir la posibilidad de ocurrencia o impactos derivados de una posible explotación de la vulnerabilidad

Posibles precursores de incidentes de acceso no autorizado	
Acción	**Respuesta**
Los usuarios reportan posibles actividades de ingeniería social	Se debe remitir una alerta a todos los usuarios alertándolos sobre las técnicas de ingeniería social y como protegerse de esos ataques. El grupo de respuesta a incidentes debe identificar los recursos a los que estaba dirigido el ataque para establecer el posible objetivo final del atacante e implementar medidas de prevención.
Una persona o sistema identifica un intento fallido de acceso físico (individuos ajenos al INSTITUTO PARA LA ECONOMIA SOCIAL intentando ingresar a áreas seguras o intentando tener acceso a equipos)	Si es viable el área de seguridad del INSTITUTO PARA LA ECONOMIA SOCIAL debe retener al posible atacante para identificar las razones por las cuales intenta acceso no autorizado, si no hay explicación razonable se debe informar a las autoridades pertinentes para proceder de acuerdo a la ley. Se deben verificar los controles del áreas físicas para determinar la fortaleza de los mismos y mejorarlos dado el caso.

Posibles indicadores de incidente de acceso no autorizado	
Acción malicioso	**Posibles indicadores**

Se compromete la cuenta de superusuario de un servidor	• Existencia de herramientas de análisis de seguridad o explotación de vulnerabilidades no autorizadas en servidores
	• Tráfico inusual hacia y desde un servidor
	• Cambios en la configuración del servidor
	  • cambios en servidores, puertos, registros de arranque y parada de servidores, cambios en políticas o datos
	  • interfaces de red configuradas en modo

Posibles indicadores de incidente de acceso no autorizado	
Acción malicioso	**Posibles indicadores**
	promiscuo • cambios en los niveles de privilegios de usuarios o grupos • Modificaciones a archivos críticos, estampas cronológicas y privilegios en archivos ejecutables, Kernel de sistema operacional, librerías del sistema, archivos de datos y de configuración. • Cambio no justificado en el uso de una cuenta (períodos prolongados de inactividad, uso de cuentas desde múltiples lugares físicos al mismo tiempo, comandos inusuales desde la cuenta de usuario, elevado número de cuentas bloqueadas) • Cambios significativos en el uso de recursos (CPU, Red, memoria, archivos del sistema, archivos de registro de actividad llenos) • Usuarios que reportan no disponibilidad del sistema • Alertas del IDS/IPS • Archivos nuevos con nombre inusuales (caracteres binarios, espacios intermedios, puntos iniciales) • Archivos de reportes de evento en el sistema operacional de tamaños muy grandes • El atacante llama a la entidad para informar que la está atacando
Modificaciones de datos no autorizados (servidor de página web, servidores de transferencia de archivos)	• Alertas del IDS/IPS • Incremento injustificado de la utilización de recursos • Los usuarios reportan modificación de dato • Modificaciones de archivos críticos • Archivos nuevos con nombre inusuales (caracteres binarios, espacios intermedios, puntos iníciales) • Cambios inesperados e injustificados en el uso de la CPU,memoria o filesystems
Uso no autorizado de una cuenta estándar de usuario	• Intentos de acceso a archivos críticos • Cambio no justificado en el uso de una cuenta (períodos prolongados de inactividad, uso de cuentas desde múltiples lugares físicos al mismo tiempo, comandos inusuales desde la cuenta de

Posibles indicadores de incidente de acceso no autorizado	
Acción malicioso	**Posibles indicadores**
	usuario, elevado número de cuentas bloqueadas) • Los registros del web proxy detectan descargas de software no autorizado.
Intrusión física	Los usuarios reportan no disponibilidad de redes o sistemas Cambios en el estado de servicios o equipos Guía para la gestión de incidentes de acceso no autorizado (parada, arranque, caídas) Hardware perdido (parcial o completamente). Por ejemplo desaparece una parte de un equipo. Se detecta equipos no autorizados conectados a la red: portátiles, smartphones, tabletas, teléfonos
Acceso no autorizado a datos (bases de datos, archivos de claves)	IDS/IPS genera alertas sobre intento de acceso no autorizado a datos mediante protocolos como HTTP, FTP.

9.5 Contención, Erradicación y Recuperación

Además de las acciones genéricas del procedimiento de respuesta a incidentes, se debe realizar las siguientes acciones particulares para la respuesta a incidentes de acceso no autorizado.

9.5.1 Selección de estrategia de contención

El tiempo de respuesta en incidentes de acceso no autorizado es de naturaleza crítica, un análisis detallado de la situación puede tomar mucho tiempo y la situación puede cambiar rápidamente. La respuesta específica en cada caso depende de la situación pero una combinación de las siguientes acciones debe ser evaluada por el grupo de respuesta a incidentes.

Aislar el sistema comprometido: Lo más simple es desconectar el sistema de la red, pero se deben tomar todas las medidas de mitigación para alerta a los usuarios. Se debe identificar y verificar que sistemas fueron afectados antes de proceder a su aislamiento, es posible que se estén usando sistemas internos para comprometer a otros sistemas y en esos casos se deberá aislar más de un sistema.

Deshabilitar los servicios afectados: Si el análisis detecta que el atacante está haciendo uso de un servicio, la medida de contención inmediata es deshabilitar el

servicio comprometido.

Eliminar la ruta de ataque hacia el servicio/servidor: Si es posible se debe aislar los segmentos de red o redes virtuales que están comprometidas para impedir que el ataque se mueva a otros recursos cercanos al servidor comprometido.

Deshabilitar las cuentas de usuario que ha sido empleadas para el ataque: Si existen más cuentas de usuario con el mismo nombre o peor aún con el mismo password se debe proceder a deshabilitar esas cuentas en todos los servidores en donde existan. Si el atacante creo nuevas cuentas de acceso estas también debe ser deshabilitadas.

Reforzamiento de la seguridad física: si el incidente incluyó uso de brechas a la seguridad física, es necesario reforzar todas las medidas de seguridad física.

9.5.2 Recolección y manejo de evidencias

Si se sospecha de un incidente de acceso no autorizado, se debe proceder a realizar una imagen forense de los sistemas comprometidos. Otros datos que deben ser recolectados son: logs de servidores, aplicaciones, IDS/IPS, Firewall. Si el incidente contemplo seguridad física se debe asegurar evidencias como registro de ingreso de visitantes, vídeos de las cámaras de vigilancia, registro de ingreso a centro de cómputo. Los incidentes de acceso no autorizado son más susceptibles a acciones legales, por esa razón la recolección de evidencia y el reporte a la autoridades competentes debe realizarse de acuerdo con los lineamientos del código de policía.

9.5.3 Erradicación y recuperación

Debido a que los ataques de acceso no autorizado contemplan en la mayoría de los casos la instalación de rootkit para alterar el comportamiento del sistema operacional, en los casos en donde el superusuario fue comprometido se debe:

- Considerar que el servidor ya no es seguro y se realizar la reinstalación del sistema operacional y de las aplicaciones con una copia limpia.
- Proceder al aseguramiento del servidor.
- Cambiar todos los password de acceso
- Ejecutar un análisis de vulnerabilidades sobre los sistemas comprometidos y cerrarlas.

En los casos en que el incidente no haya comprometido el superusuario se debe:

- Cerrar las vulnerabilidades detectadas de acuerdo con la extensión del ataque.
- Cambiar las claves comprometidas y reforzar la política de claves seguras

- Proceder al aseguramiento del servidor.
- Ejecutar un análisis de vulnerabilidades sobre los sistemas comprometidos y cerrarlas.

Lista de chequeo de respuesta a incidentes de acceso no autorizado
Advertencia: Los pasos de la lista de chequeo pueden variar en orden de acuerdo con la naturaleza del ataque. Es responsabilidad del [oficial o encargado de seguridad de la información], coordinar las actividades de respuesta al incidente.

Lista de chequeo de respuesta a incidentes de acceso no autorizado		
Paso	**Acción**	**Completada**
Análisis		
1	Priorizar el manejo del incidente de acuerdo con el impacto para la función misional del INSTITUTO PARA LA ECONOMIA SOCIAL	
1.1	Identificar que recursos han sido afectados y estimar que recursos podrían ser afectos	
1.2	Estimar el impacto real y potencia del incidente	
1.3	Identificar en la matriz de impacto el nivel de prioridad del incidente	
2	Reportar el incidente a la instancias pertinentes	
Contención, erradicación y recuperación		
3	Realizar contención preliminar del incidente	
4	Recopilar, Preservar, asegurar y documentar la evidencia	
5	Confirmar la contención del incidente	
5.1	Analizar el incidente para determinar si la medida de contención fue suficiente (extender el análisis a otros sistemas para identificar signos de acceso no autorizado)	
5.2	Implementar medidas complementarias de contención si es necesario.	
6	Erradicar el incidente	
6.1	Identificar y mitigar las vulnerabilidades explotadas	
6.2	Remover los componentes del ataque de los sistemas afectados	

Lista de chequeo de respuesta a incidentes de acceso no autorizado		
Paso	**Acción**	**Completada**
7	Recuperación del incidentes	
7.1	Retornar los sistemas afectados a estado operacional	
7.2	Confirmar que los sistemas operan correctamente	
7.3	Si es necesario implementar medidas adicionales de supervisión	
Revisión post incidente		
8	Crear un reporte de seguimiento del incidente	
9	Realizar la sesión de lecciones aprendidas	

Anexo G

10 GUÍA DE ATENCIÓN DE INCIDENTES DE USO INAPROPIADO

10.1 Definiciones

Un incidente de uso inapropiado ocurre cuando un usuario realiza acciones que incumplen las políticas de seguridad de la información del INSTITUTO PARA LA ECONOMIA SOCIAL. Aunque en la mayoría de las veces estos incidentes no comprometen la seguridad del INSTITUTO PARA LA ECONOMIA SOCIAL se debe responder a ellos en forma similar a los demás.

Algunas situaciones que se consideran incidentes de seguridad de uso in apropiado incluyen pero no se limitan a:

- Descarga de software sin autorización del [oficial o encargado de seguridad de la información]
- Descarga o acceso a material pornográfico o material prohibido por ley (terrorismo, segregación racial, etc.)
- Uso del correo electrónica para enviar correo masivo no deseado o promover negocios personales
- Envío de correos intimidatorios, ofensivos o agresivos al personal de INSTITUTO PARA LA ECONOMIA SOCIAL
- Uso de servicios de archivo compartido para intercambiar música, vídeos, software o todo material protegido por derechos de autor.
- Transferir información de propiedad de la entidad sin autorización a terceros.
- Demás acciones no autorizadas por las políticas, normas o procedimientos del INSTITUTO PARA LA ECONOMIA SOCIAL.

10.2 Preparación

Está sección describe acciones específicas para manejar incidentes de seguridad uso inapropiado

10.2.1 Preparación para el manejo del incidente

Además de las acciones generales descritas en el procedimiento de respuesta a incidentes se deben realizar las siguientes actividades:

Realizar una reunión con el área de recursos humanos y área jurídica para determinar el manejo que se dará a los incidentes de uso inapropiado de recursos.

Supervisar las actividades de los usuarios para verificar que se cumplen las políticas de seguridad.

Debido a que los incidentes contemplan a empleados, funcionarios o contratistas del INSTITUTO PARA LA ECONOMIA SOCIAL se debe mantener la confidencialidad del incidente debido a que el incidente puede ser la base para procesos legales o disciplinarios.

Realizar reuniones con el área de seguridad del INSTITUTO PARA LA ECONOMIA SOCIAL para determinar procedimientos de manejo de personas que reaccionen violentamente en caso de que sean detectados en actividades que contravienen las políticas de seguridad.

Configurar el software de IDS, filtrado de contenido y los controles de seguridad para que identifiquen ciertos tipos de actividad como:

- Usuarios empleando servicios no autorizados cono protocolos peer-to-peer y música compartida
- envío de correo masivo
- Actividad sospechosa como: adjuntos de gran tamaño en correo, transferencia de archivos por FTP, solicitudes de acceso a páginas wen registradas en listas negras.

Registrar las actividades de los usuarios como transferencia de archivos, acceso a páginas web y encabezamientos de correos, usando las herramientas del web proxy o el IDS.

10.2.2 Prevención del incidente

Las acciones para prevenir el uso indebido de recursos incluyen:

- Formación y toma de conciencia a los usuarios
- Divulgación de políticas de seguridad
- Clausulas en los contratos que autorizan al INSTITUTO PARA LA ECONOMIA SOCIAL a supervisar el uso de los recursos como correo, servidores de archivos y computadores personales suministrados por la entidad.
- Informar a los usuarios que por su seguridad sus actividades son supervisadas
- Configurar los firewall, proxy e IDS para controlar y supervisar el uso de recursos y verificar el cumplimiento de las políticas de seguridad.
- Configurar el servidor de correo del INSTITUTO PARA LA ECONOMIA SOCIAL para impedir su uso como Open-relay
- Implementar filtros antispam

- Implementar el filtrado de contenido para impedir el acceso a sitios web no autorizados
- Restringir el uso de protocolos cifrados como SSH, HTTPS e Ipsec solo a los debidamente autorizados y a los sitios debidamente aprobados.

10.2.3 Detección y análisis

Las labores de detección de actividades de uso inapropiado se basan en la revisión de reportes de uso. La siguiente tabla describe los posibles indicadores de uso inapropiado.

Posibles indicadores de incidentes de uso inapropiado	
Acción de uso inapropiado	**Posible indicador**
Uso no autorizado de un servicio (web server, página web, uso compartido de archivos protegidos por derechos de autor)	Alertas del software supervisión de red Tráfico inusual que proviene del servidor Procesos nuevos ejecutándose en el servidor sin razón aparente Nuevos directorios creados con nombres asociados a servicios como wares Incremento en el uso de CPU, disco, red o memoria registros en las aplicaciones de supervisión (Web proxy, servidor de correo, IDS)
Acceso a material no autorizado (ej. pornografía, spam)	Alertas del web proxy y software de IDS Reportes de usuario Archivos inapropiados en las estaciones de trabajo, servidores o medios removibles.

10.2.4 Contención, erradicación y recuperación

El manejo de incidentes de uso inapropiado por lo regular no contempla estrategias de contención, erradicación o recuperación, la mayoría de las veces se debe borrar el material objeto del uso inapropiado o desinstalar el software no autorizado. La recolección de evidencia debe ser más cuidadosamente porque puede ser parte de procesos legales o disciplinarios. De igual forma se debe asegurar con mayor precisión la evidencia porque los usuarios implicados pueden intentar su eliminación para evitar sanciones.

Lista de chequeo para manejo de incidentes de uso inapropiados		
Paso	**Acción**	**Completa**
Detección y análisis		
1	Priorizar el manejo del incidente de acuerdo con el impacto para la función misional del INSTITUTO PARA LA ECONOMIA SOCIAL	
1.1	Identificar que recursos han sido afectados y estimar que recursos podrían ser afectos	
1.2	Estimar el impacto real y potencia del incidente	
1.3	Identificar en la matriz de impacto el nivel de prioridad del incidente	
2	Reportar el incidente a la instancias pertinentes	
Contención, erradicación, recuperación		
3	Recopilar, Preservar, asegurar y documentar la evidencia	
4	Si es necesario contener y erradicar el incidente removiendo el material inapropiado.	
Revisión post incidente		
5	Crear un reporte de seguimiento del incidente	
6	Realizar reunión de lecciones aprendidas	

Anexo H

11 GUÍA PARA LA GESTIÓN DE INCIDENTES MULTICOMPONENTE

11.1 Definición

Un incidente de multicomponente es un aquel que contempla dos o más incidentes. Un ejemplo de esta situación puede ser:

1. Un código malicioso se propaga por el correo y compromete una estación de trabajo.

2. Un atacante (que puede ser o no el que envió el código malicioso) usa la estación infectada

3. El atacante (que puede ser el mismo u otro diferente a los ataques anteriores) usa un servidor comprometido para lanzar un ataque de DoS en contra de otra entidad.

En un caso de incidente multicomponente la fase de análisis debe ser muy precisa.

11.2 Preparación, detección y análisis

Debido a que un incidente de este tipo implica relación de varios incidentes, el grupo de respuesta a incidentes debe verificar la correlación de eventos, verificar los registros de errores y actividades y tratar de identificar, en lo posible, todos los componentes del ataque. Dentro del análisis se debe considerar análisis de información de los días o semanas previas a la fecha de identificación del incidente. En el caso de incidentes multicomponente se deben seguir los pasos del análisis de los tipos de incidentes que conforman el incidente compuesto.

11.2.1 Contención, Erradicación y recuperación

Debido a que puede ser muy complejo identificar a primera vista los componentes de este incidente, lo mejor es responder al incidente detectado y luego buscar síntomas de la existencia de otros incidentes ir tratando cada incidente. El grupo de respuesta a incidentes debe entrenarse en la identificación de síntomas de incidentes multicomponente. Cada incidente detectado debe ser priorizado en su atención para evitar que todo el grupo de atención a incidentes se concentre en un solo incidente.

Lista de chequeo para incidentes multicomponente

La siguiente lista describe los pasos de alto nivel para la atención de incidentes multicomponente, la lista se debe complementar con las acciones específicas cada componente del incidente y las acciones genéricas del procedimiento de respuesta

a incidentes.

Lista de chequeo para incidentes multicomponente		
Paso	**Acción**	**Completado**
Análisis		
1	Priorizar el manejo del incidente de acuerdo con el impacto para la función misional del INSTITUTO PARA LA ECONOMIA SOCIAL	
1.1	Identificar que recursos han sido afectados y estimar que recursos podrían ser afectos	
1.2	Estimar el impacto real y potencia del incidente	
1.3	Identificar en la matriz de impacto el nivel de prioridad del incidente	
2	Reportar el incidente a la instancias pertinentes	
Contención, erradicación y recuperación		
3	Seguir los pasos de Contención, erradicación y recuperación de cada componente del incidentes de acuerdo con los resultados del pasos 1	
Revisión Post incidente		
4	Crear un reporte de seguimiento del incidente	
5	Realizar reunión de lecciones aprendidas	

11.2.2 Recomendaciones para incidentes multicomponentes

- Se debe configurar un servidor centralizado para recolección de registros de las diferentes herramientas de diagnóstico y usar software de correlación de eventos.

- Se debe contener el incidente inicialmente priorizado y buscar síntomas de otros componentes de incidente

- Separadamente priorizar la gestión de cada componente del incidente.

12 DOCUMENTOS ASOCIADOS

- Procedimiento de Manejo de Incidentes de Seguridad.

13 CONTROL DE CAMBIOS

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