SE APRUEBA PARA EL INSTITUTO DE PREVISIÓN SOCIAL, EL INSTRUCTIVO INSTITUCIONAL DENOMINADO "PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN"

RESOLUCIÓN EXENTA Nº 316

SANTIAGO, 01 JUL 2016

VISTOS:

1.- La Ley N° 20.255, de Reforma Previsional, que establece la nueva Institucionalidad Pública para el Sistema de Previsión Social y crea entre sus órganos, el Instituto de Previsión Social determinando sus funciones y atribuciones; y el D.F.L. N° 4, de 2009, del Ministerio del Trabajo y Previsión Social que fija la Planta de Personal y fecha de iniciación de actividades de este Instituto.

2.- El D.F.L.N°1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fijó el texto refundido, coordinado y sistematizado, de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

3.- La Ley N° 19.880, de Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado.

4.- El D.F.L. N° 278, de 1960, del Ministerio de Hacienda; el D.L. N° 49, de 1973; el D.F.L. N° 17, de 1989, del Ministerio del Trabajo y Previsión Social; la Resolución N° 1600, de 2008, de la Contraloría General de la República, que fijó las normas sobre exención del trámite de toma de razón; y las facultades que me concede el artículo 57°, de la Ley N° 20.255.

CONSIDERANDO:

1.- Que, resulta necesario establecer las actividades del Instituto de Previsión Social, para la detección oportuna y el tratamiento de debilidades o eventos que han sido categorizados como incidentes de seguridad de la información, que afecten a los activos de información del tipo: base de datos, documento, equipo, expediente, formulario, infraestructura física, persona, sistema de información, software, en cuanto a: confidencialidad, integridad y disponibilidad de la información, ya que comprometen la provisión de bienes y servicios por parte de la institución.

2.- Que, para la aplicación general y obligatoria del citado procedimiento, el Departamento de Seguridad de la Información dependiente de la División Informática del Instituto de Previsión Social, ha elaborado el Instructivo Institucional denominado "Procedimiento de Gestión de Incidentes de Seguridad de la Información".

3.- Que, por Oficio Ordinario Nº 45338/2729-16, de 08 de junio de 2016, la División Jurídica de este Instituto, emite informe sobre la aprobación legal del instructivo de la especie, estableciendo la procedencia de dictar la correspondiente resolución aprobatoria por el Departamento de Transparencia y Documentación, la que de conformidad a las disposiciones contenidas en la Resolución N°1600, de la Contraloría General de la República, de 2008, que fija normas sobre exención del trámite de Toma de Razón, se encuentra exenta del mencionado trámite.

R E S U E L V O:

1.- **Apruébase** para el Instituto de Previsión Social, el Instructivo denominado "Procedimiento de Gestión de Incidentes de Seguridad de la Información", que consta de veintinueve (29) páginas, que se adjunta como parte integrante de la presente Resolución Exenta, con aprobación legal de fecha 08 de junio de 2016, cuyo objetivo es establecer las actividades del Instituto de Previsión Social, para la detección oportuna y el tratamiento de debilidades o eventos que han sido categorizados como incidentes de seguridad de la información, ya que comprometen la provisión de bienes y servicios por parte de la institución.

2.- Publíquese el Procedimiento, que se aprueba por el presente acto administrativo, en el ambiente "Instructivos Institucionales", de la Intranet del IPS.

3.- Cúmplase con lo dispuesto en el artículo 48, de la Ley Nº 19.880, citada en Vistos Nº 4 y en el Instructivo Presidencial Gab. Pres. Nº 008, de 04 de diciembre de 2006, complementado por Circular Conjunta Nº 3, de 05 de enero de 2007, del Ministerio del Interior y Ministerio de Hacienda, en orden a publicar un extracto del presente acto administrativo en el Diario Oficial y texto completo del mismo en el Banner "Gobierno Transparente".

Notifíquese, regístrese y distribúyase por Departamento de Transparencia y Documentación, a las Jefaturas de las unidades incluidas en la Distribución de la presente Resolución.

INSTITUTO DE PREVISIÓN SOCIAL

PATRICIO CORONADO ROJO
DIRECTOR NACIONAL
DIRECTOR NACIONAL
INSTITUTO DE PREVISIÓN SOCIAL

DISTRIBUCION:
- Gabinete Dirección Nacional
- Subdirección de Servicios al Cliente
- Subdirección de Sistema de Información y de Administración
- División Jurídica
- División Contraloría Interna
- División Beneficios
- División Canales de Atención a Clientes
- División Informática
- División Planificación y Desarrollo
- Departamento Personas
- Departamento Finanzas
- Departamento Administración e Inmobiliaria
- Departamento Transparencia y Documentación
- Departamento Cobranza Institucional
- Departamento Comunicaciones
- Departamento Auditoría Interna
- Direcciones Regionales IPS
- Subdepartamento de Tesorería
- Unidad de Apoyo Documental División Jurídica

MEES/AOA/MCM/ VCG/MVEW/ NCR/RPV/ MRC/mrc
Instructivo "Procedimiento de Gestión de Incidentes de Seguridad de la Información".
VI- (Folio DTD/3575-61-20)

PROCEDIMIENTO DE GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Elaborado por:	Revisado por:	Aprobado por:
Departamento de Seguridad de Información	Encargada de Seguridad de la Información	División Jurídica Dirección Nacional

CONTROL DE CAMBIOS

Fecha	Versión	Página	Numeración del contenido	Cambio Efectuado/Nombre del responsable
0x/xx/2016	01			Versión inicial del documento

La presente versión sustituye completamente a todas las precedentes, de manera que éste sea el único documento válido de entre todos aquellos sobre la materia.

NOTA DE ENFOQUE DE GÉNERO

El uso de un lenguaje que no discrimine ni marque diferencias entre hombres y mujeres ha sido una preocupación en la elaboración de este documento. Sin embargo, y con el fin de evitar la sobrecarga gráfica que supondría utilizar en español o/a para marcar la existencia de ambos sexos, se ha optado por utilizar el masculino genérico, en el entendido de que todas las menciones en tal género representan siempre a todos/as, hombre y mujeres, abarcando claramente ambos sexos.

NOTA DE CONFIDENCIALIDAD

La información contenida en este documento es de propiedad del Instituto de Previsión Social y debe ser tratada de acuerdo a su nivel de confidencialidad, sobre la base de las instrucciones establecidas en la política de clasificación y manejo de información. El uso no autorizado de la información contenida en este documento podrá ser sancionado de conformidad con la ley chilena. Si usted ha recibido este documento por error, le pedimos eliminarlo y avisar inmediatamente al Instituto de Previsión Social (IPS).

INDICE

1. OBJETIVO

Establecer las actividades necesarias del Instituto de Previsión Social, para la detección oportuna y el tratamiento de debilidades o eventos que han sido categorizados como incidentes de seguridad de la información, ya que comprometen la provisión de bienes y servicios por parte de la institución.

2. ALCANCE

Este procedimiento es aplicable a todos los funcionarios (planta, contrata, reemplazos), personal a honorarios y terceros (proveedores, compra de servicios), que presten servicios al IPS.

Es aplicable a los incidentes de seguridad de la información, que afecten a los activos de información del tipo: base de datos, documento, equipo, expediente, formulario, infraestructura física, persona, sistema de información, software, en cuento a:

- Confidencialidad: acceso no autorizado a la información.
- Integridad: modificación no autorizada, destrucción o perdida de información.
- Disponibilidad: inaccesibilidad a la información.

	PROCEDIMIENTO DE GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			DIVISION DE INFORMATICA
	Nivel de Confidencialidad	Uso Interno	Versión	01
			Fecha de Aprobación Legal	08 JUN 2016
			Página	5 de 29

3. DOCUMENTOS DE REFERENCIA

- Resolución Exenta N ° 657, 03/12/2015, define Política General de Seguridad de la información IPS.
- Resolución Exenta N° 320, 19/07/2012; establece estructura orgánica del Instituto de Previsión Social
- Resolución Exenta N° 231, 24/02/2014, fija la estructura orgánica interna de la división informática
- Resolución Exenta N° 223, 18/05/2016, aprueba la "Política de Gestión de Incidentes de Seguridad de la información" inserta en el sistema de seguridad de la información del IPS.
- Resolución Exenta N°170, del 10 de abril de 2015, que designó al Encargado de Seguridad de la Información
- Resolución Exenta N°56, 15/02/2016, Política Organizacional de la Seguridad de la Información del IPS.
- Norma NCh- ISO 27000:2013
- Norma NCh-ISO 27001:2013,
    - A.16.1.1 Responsabilidades y procedimientos

4. DEFINICIONES

a) **Activo de Información (ADI)**: Elementos más relevantes para la producción, el procesamiento, la emisión, el almacenaje, la comunicación, la visualización, los encargados y la recuperación de la información que tiene un elevado valor para la organización. Pueden clasificarse en personas, sistemas, hardware e infraestructura.

b) **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

c) **Debilidades en la seguridad de la información:** Debilidad de un activo o de un grupo de activos que puede ser explotada por una o más amenazas que pueden poner en riesgo la seguridad de la información.

d) **Escalar Problemática**: Acción que opera cuando el equipo de incidentes no es capaz de resolver en primera instancia un incidente, por lo cual es necesario recurrir a un especialista o superior que tome decisiones que escapan a su responsabilidad.

e) **Comité de Seguridad de la Información (CSI):** Grupo integrado por las Jefaturas de la División, y ciertas Jefaturas de Departamentos, Presidido por el (la) Encargado(a) de seguridad de la información, cuyo objetivo es tomar decisiones respecto a temas y políticas de seguridad de la información.

f) **Evento de seguridad de la información:** Aparición identificada del estado de un sistema, servicio o red que indica una posible violación de las políticas de seguridad de la información o la falta de salvaguardias o una situación previamente desconocida que puede ser pertinente a la seguridad.

g) **Gestión incidente de seguridad de la información:** Procesos para detectar, comunicar, evaluar, responder, hacer frente a, y aprender de incidentes de seguridad de la información.

h) **Incidente de seguridad de la información:** Situación adversa que amenaza o pone en riesgo un proceso en el que existan tratamiento de datos, independientemente de su grado de confiabilidad.

i) **Jefatura**: Funcionario encargado de un grupo de personas, conformados en, Unidad, Departamento, Área, o División.

j) **Recogida de Datos:** Acción realizada al registrar los datos en el formulario de incidentes de seguridad.

V°B° DEPTO. CONTROL JURIDICO I.P.S.

5. RESPONSABILIDADES

a) **Comité de Seguridad de la Información (CSI):** Grupo responsable ante la Dirección Nacional por la existencia y cumplimiento de las medidas de seguridad de la información acorde con las necesidades del IPS, los recursos disponibles y la normativa vigente.

b) **Comité de Gestión de Incidente de Seguridad de la Información (CGISI)**: Equipo de miembros del IPS, con la capacidad y la confianza apropiada, que se encargará de los eventos e incidentes de seguridad de la información durante el ciclo de vida de los mismos, coordinados por el Jefe de Seguridad de Información (JDSI) de la División Informática.

c) **Departamento Desarrollo y Mantención de Sistemas (D y M) División Informática**: Responsables de gestionar y controlar la actualización y registro de las metodologías de Desarrollo y Documentación basada en estándares definidos y las buenas prácticas de Tecnología Informática Institucionales.

d) **Departamento Producción (DP) División Informática**: Responsable de administrar los diferentes sistemas de información del Instituto que se encuentren liberados y en producción, asegurando su funcionamiento en todo evento u incidente, a través de la gestión de mecanismos de respaldo y planes de recuperación ante fallas.

e) **Departamento Seguridad de Información (DSI):** Responsables de gestionar y controlar el sistema de gestión de la seguridad, sobre la protección de los activos de información del instituto, conforme a la normativa vigente y los objetivos estratégicos institucionales.

Responsables de coordinar y controlar la implantación de la infraestructura de seguridad periférica y dedicada a los servicios críticos en software, hardware y procedimientos, proponiendo a la Jefatura de la División las correcciones y mejoras necesarias, en el marco del mejoramiento permanente de la gestión.

f) **División de Informática (DI):** Responsable de dirigir, coordinar, operar y controlar el modelo de gestión de las tecnologías de información, telecomunicaciones y seguridad de la información del Instituto, debiendo proponer a la Dirección Nacional las acciones correctivas y de mejoras que correspondan y coordinar su implementación.

g) **Funcionario del IPS**: Responsable de cumplir con lo establecido en este documento y aplicarlo en su entorno laboral. Tiene la obligación de alertar de manera oportuna y adecuada por los canales y procedimientos formales establecidos, cualquier situación que pueda poner en riesgo la seguridad de la información.

h) **Encargado de Seguridad de la Información (EDSI):** Responsable de la administración, actualización, protección y control del ciclo de vida del documento.

i) **Jefe de Departamento Seguridad de Información (JDSI):** Responsable de la aplicación de este procedimiento, gestionar los eventos, debilidades e incidentes de seguridad de la información y posteriormente dirige el equipo del Departamento de Seguridad de Información.

j) **Mesa de ayuda (MAFIPS);** Recibe reporte, investiga, clasifica, contiene e informa del incidente.

k) **Centro de Operaciones de Seguridad (SOC):** Es un Centro de Operaciones destinado a dar un servicio de seguridad gestionada externaliza al Instituto de Previsión Social (IPS). Para ello debe contar con un equipo con personal especialista en varias áreas complementarias que permitan dar un servicio global y efectivo,

DIVISIÓN JURÍDICA V°B° DEPTO. CONTROL JURÍDICO I.P.S.

6. DESCRIPCIÓN DEL PROCEDIMIENTO

6.1 Descripción de Actividades

La gestión de incidentes en el IPS, debe contemplarse como un ciclo con distintas fases que incluyen desde la preparación inicial previa a la materialización de incidentes hasta las actividades de recapitulación, una vez que el IPS se ha recuperado del incidente.
Las distintas fases son las siguientes:

6.1.1. Preparación

Las actividades de preparación se inician con el establecimiento de la capacidad de respuesta a incidentes.

a) Establecimiento de procedimientos de gestión:

Los incidentes se pueden originar y materializar de maneras muy distintas. Por tanto, no es factible ni práctico desarrollar procedimientos detallados con instrucciones precisas para todos los posibles tipos de incidentes.

Asimismo, el IPS debe estar preparado para manejar de modo genérico cualquier tipo de incidente de modo eficaz y efectivo.

b) Establecimiento de capacidad de respuesta:

Una actividad previa a la puesta en marcha del Comité de Gestión de Incidente de Seguridad de la Información (CGISI) es recopilar, estructurar y almacenar la siguiente información:

- Información de contacto de los miembros del Comité de Gestión de Incidente de Seguridad de la Información (CGISI) del IPS. Se debe disponer al menos del contacto principal y el de respaldo.
- Información de contacto de otros miembros como son representantes de Divisiones, usuarios Claves o Dueños de Procesos.
- Mecanismos de recepción y escalado de incidentes: teléfonos, correo electrónico y formularios.
- Documentación de sistemas y redes: inventario de activos, diagramas, procedimientos y archivos de configuración.
- Informes de actividad considerada normal de redes y sistemas que permitan detectar actividades anómalas.

- Sala de coordinación de incidentes temporal a activar en caso necesario.
- Facilidades de almacenamiento seguro de datos para evidencias de incidentes u otra información sensible sólo accesible bajo control del equipo de gestión de incidentes.
- Estaciones de trabajo para análisis forense y/o dispositivos de respaldo para la creación de imágenes de discos, almacenamiento de logs e información relevante al incidente.
- Equipos personales tipo PC y/o Notebook para actividades de análisis, redacción de informes y comunicación.
- Herramientas de análisis de protocolos y vulnerabilidades
- Aplicaciones de análisis forense que permitan analizar imágenes de disco para obtener evidencias de incidentes.
- Accesorios que permitan recoger evidencias, tales como cámaras fotográficas, grabadores de audio y/o video.

6.1.2. Detección y Análisis

Las actividades de detección y análisis incluyen la clasificación de incidentes que pueden afectar al IPS, detección de signos y precursores de incidentes, análisis, priorización, notificación y documentación de los incidentes.

6.1.3. Detección y signos de incidentes

a) Tipos de signos de incidentes

Los signos de un incidente pueden ser de dos tipos, indicadores y precursores:

- **Indicadores**: signos de ocurrencia de un incidente o puede estar ocurriendo; ejemplo: alerta de un sensor avisando un desbordamiento de buffer en un servidor, antivirus informando de un sistema infectado, caída total de un servidor, accesos lentos generalizados a servicios, otros.

- **Precursores**: signos que evidencias que un incidente puede ocurrir en el futuro; ejemplo: barrido de puertos detectado, anuncio de "exploits" que pueden aprovechar vulnerabilidades existentes en la organización, amenazas de ataque anunciadas por hackers, otros.

Cualquier incidente presenta indicadores que pueden ser detectados con mayor o menor complejidad, pero no todos los incidentes presentan precursores. Los indicadores deberían poner en marcha acciones reactivas previstas por la organización. Los precursores deberían ser tratados con acciones preventivas.

6.1.4. Fuentes de precursores e indicadores

Algunas fuentes de precursores e indicadores que el IPS debe considerar son:

- **Alertas de software**: sistemas de detección y prevención de intrusiones IDS/IPS, antivirus, sistemas de monitorización de servicios.
- **Logs** de sistemas operativos, dispositivos de red y aplicaciones.
- **Información pública**: nuevas vulnerabilidades y "exploits", sitios Web y listas de correo de profesionales donde se comparten experiencias de incidentes en distintas organizaciones.
- **Funcionarios**: Funcionarios del IPS.

6.1.5. Análisis de incidentes

Dada la complejidad de la realización del análisis y validación de incidentes, es necesario formalizar, como mínimo, las siguientes actividades de análisis y gestión de incidentes.

a) **Perfilar las redes y sistemas:** Se deben establecer las características de la actividad normal de las redes y sistemas del IPS. De este modo, se pueden detectar cambios que puedan ser indicadores o precursores de incidentes.

b) **Conocer comportamientos normales**: Se deben estudiar y establecer las situaciones que deben ser consideradas como comportamientos normales de los sistemas, redes y aplicaciones. De este modo, se pueden reconocer comportamientos no normales que pueden ser signos de incidentes.

c) **Centralizar, correlacionar y conservar información de logs:** Se cuenta con un servidor donde se consolida, correlaciona y conserva copias de los archivos de logs de los distintos sistemas de la organización como cortafuegos, dispositivos de comunicaciones, servidores y sistemas de detección o prevención de intrusiones.

Se utilizan herramientas para el análisis y correlación de logs y se definirá la política de conservación de logs, de modo que se conserven las evidencias de posibles incidentes.
Mantener sincronizados los relojes de los servidores.

Se implementarán los mecanismos necesarios para mantener sincronizados los relojes de todos los servidores de la organización. Esto es importante para la correcta correlación y análisis de incidentes.

d) **Crear o Armar una base de conocimientos:** Se debe establecer una base de conocimientos, que incluya la información necesaria para la gestión de incidentes.

Los contenidos a incluir, como mínimo, son:

- Enlaces a información sobre amenazas, vulnerabilidades, exploits o virus
- Dominios o direcciones IP bloqueadas por ser fuente de spam o ataques
- Explicación de signos de incidentes con origen en sistemas de detección de intrusiones y logs de equipos
- Información sobre códigos de error de sistemas y aplicaciones
- La base de conocimientos será accedida y actualizada por todos los miembros del Comité de Gestión de Incidente de Seguridad de la Información (CGISI).

e) **Definir niveles de filtrado de signos de incidentes:** Cuando el volumen de información relativa a incidentes potenciales es muy elevado, no es posible analizar toda la información recogida. Se deberán establecer niveles de filtrado, de modo que solo la información más relevante sea resaltada y analizada por el equipo de gestión de incidentes. Esta medida evita que el exceso de información, pueda camuflar o hacer pasar desapercibidos signos de incidentes importantes.

6.1.6 Acciones posteriores al incidente, cierre y recapitulación

Una vez que se han realizado las tareas de detección, análisis, contención y recuperación del incidente y la organización haya vuelto a la situación de operación normal es necesario realizar las siguientes acciones de recapitulación y cierre.

a) Análisis de recapitulación y lecciones aprendidas

Se hará un estudio de recapitulación analizando las características de los incidentes, impacto y acciones emprendidas para la detección, análisis y recuperación.

- En incidentes menores es suficiente con completar un formulario que describa los elementos anteriores e incluya origen o persona que detecta el incidente, sistemas afectados, fecha, hora y responsable de la gestión del incidente.
- En incidentes mayores, el equipo de gestión de incidencias debe reunirse una vez realizada la contención y recuperación del incidente, para analizar las actividades realizadas y estudiar posibles mejoras o cambios que deban realizarse ante futuros incidentes.

Para esta reunión se convocará a todos los miembros del equipo de gestión de incidentes, Encargado de Seguridad de la Información, responsable de sistemas, responsable de redes y representantes de los servicios o departamentos afectados por el incidente.

Los elementos que han de analizarse en la **Reunión de Lecciones Aprendidas** son:

- Acciones realizadas de análisis de síntomas y detección del incidente.
- Acciones realizadas para la calificación del incidente, determinación de impacto previsible y priorización.
- Acciones emprendidas por el equipo de gestión, personal de la organización o terceras partes.
- Información que se utilizó en la gestión del incidente.
- Información que hubiera sido útil y no estaba disponible.
- Posibles acciones emprendidas con resultado nulo o negativo.
- Recursos humanos y técnicos empleados para la resolución del incidente.
- Recursos adicionales considerados necesarios para la resolución de futuros incidentes.
- Acciones correctivas o preventivas que puedan emprenderse para ayudar a prevenir incidentes similares en el futuro o mejorar su gestión.
- Mejoras a realizar en los procedimientos de gestión de incidentes en base a las lecciones aprendidas.

Se redactará un informe de cierre que documentará los detalles del incidente y las acciones de gestión desarrolladas y que servirá asimismo como acta de la reunión de recapitulación y lecciones aprendidas.

- **Acciones legales**: si se emprenden acciones legales dirigidas contra el causante del incidente, puede ser necesario retener las evidencias hasta que las acciones legales hayan terminado. Debe considerarse también, que evidencias que pueden parecer insignificantes al iniciar las acciones, pueden resultar ser importantes en el futuro. Es importante considerar una cadena de custodia adecuada para las evidencias puedan tener valor legal.
- **Políticas de retención de datos**: la política de retención de datos o requerimientos legales de conservación, puede requerir extender el tiempo de retención especificado o reglamentado si los datos son evidencias de incidentes importantes.
- **Costo**: se debe considerar el costo de retención de datos en soportes magnéticos como discos duros y la necesidad de mantener dispositivos que puedan realizar su lectura.

b) Documentación de incidentes

En el momento que el Departamento de Seguridad de Información (DSI), sospecha que ha ocurrido o puede estar ocurriendo un incidente de seguridad, empezarán a recoger todos los hechos relativos al incidente.

Los medios de registro pueden ser manuales, como un cuaderno de registro de incidentes y electrónicos, como Smartphones, cámaras digitales, computadores personales o grabadores de audio. Se registrará toda la información considerada relevante para el análisis, solución y recapitulación del incidente.

Se registrarán todos los pasos realizados en la gestión del incidente, incluyendo todos los documentos y evidencias relativos al incidente.

Se mantendrá la base de datos de incidentes donde se registrará el estado actual del incidente y la información relativa a las diferentes fases de análisis, solución y recapitulación.

c) Estados de los incidentes

Con el objeto de tener una visión rápida de la etapa en que se encuentra un incidente, este deberá clasificarse de acuerdo a la siguiente nomenclatura:

- **Abierto**: El incidente ha sido notificado y está en conocimiento y análisis del personal de seguridad.
- **En Proceso**: se está dando respuesta al incidente, por parte del Grupo de Respuesta del Incidente.
- **Suspendido**: Se está esperando un evento, para seguir con la gestión del incidente y cuya consecución no depende de una acción concreta del Departamento de Seguridad de Información (DSI):
- **Seguimiento**: Se está realizando un seguimiento de la normalidad operativa de los sistemas afectados.
- **Cerrado**: Se ha constatado la normalidad de los sistemas afectados y se da por cerrada la gestión del incidente.

6.1.7 Denuncia a cuerpos de investigación policial

Un elevado número de incidentes, no derivan en responsabilidades para el atacante por la falta de denuncia de los mismos. Asimismo, la posible cobertura de activos asegurados puede depender de realizar la comunicación y denuncia en los tiempos y plazos requeridos.

En incidentes que puedan tener un impacto significativo en el negocio de la organización y sean originados por un ataque deliberado contra los activos del IPS, el equipo de gestión de incidentes debe contactar al cuerpo policial considerado más adecuado para realizar la denuncia del ataque.

Si existen diversos cuerpos policiales con competencia en los delitos informáticos, se debe informar al cuerpo considerado más adecuado para realizar la investigación. No se recomienda informar a más de un cuerpo policial, para evitar problemas derivados de conflictos de jurisdicción o competencias cruzadas. Se debe tener en cuenta, que el lugar de materialización del ataque no corresponde necesariamente al lugar de origen del mismo.

El contacto con los cuerpos policiales lo hará el (la) **Encargado(a) de Seguridad del Instituto de Previsión Social (IPS)** por poseer el conocimientos del modo de operar de los distintos cuerpos policiales y será quien actúe de punto principal de contacto para la investigación.

El **Comité de Gestión de Incidente de Seguridad de la Información (CGISI)** descrito en este procedimiento realizará, si procede, las acciones requeridas para la resolución del incidente, coordinando sus actuaciones con el responsable del plan de contingencias de la organización.

6.1.8 Comité de Gestión de Incidente de Seguridad de la Información (CGISI)

El CGISI es el grupo responsable de recibir, revisar y responder frente a notificaciones o descubrimientos de incidentes de seguridad. Este grupo está formalmente constituido, pero los miembros son a tiempo parcial, ya que el CGISI se activa y reúne para tratar incidentes de seguridad en curso o inminentes.

Una vez detectado un posible incidente, el CGISI califica los datos del incidente y pone en marcha los mecanismos para limitar el impacto y restaurar la situación normal previa al incidente.

El CGISI, la forma y procedimientos de contacto debe ser conocido y estar accesible a todos los miembros del IPS, de modo que sea posible la comunicación de incidentes de seguridad por cualquier miembro que detecte un posible incidente de seguridad, por lo que se requiere que se informe en los diferentes planes de difusión al interior del IPS.

Organización del CGISI

Se establece un Modelo centralizado, es decir, se genera el CGISI para todas las incidencias del IPS. El personal del CGISI debe tener las siguientes características:

- Disponibilidad 24x7.
  - Las personas designadas del CGISI tienen que poder ser localizables 24x7 y en caso de ser necesario, apersonarse en las dependencias de las oficinas

- Miembros a tiempo completo y parcial.

  - Los miembros del CGISI pueden estar asignados a otra función a tiempo parcial mientras no sea necesaria la activación del equipo. Sin embargo debe existir al menos un miembro que actúe como responsable del equipo y cuya responsabilidad y función principal en la organización sea la gestión de incidentes de seguridad.

- Experiencia en seguridad y gestión de incidencias
  - La experiencia y conocimientos del personal asignado al CGISI deben contemplar el ámbito técnico y organizativo de los sistemas y redes existentes en la organización.

- Formación
  - El equipo de gestión de incidentes idealmente debe tener formación en herramientas de análisis de vulnerabilidades y análisis forense.

6.2 Diagrama de Flujo

6.2.1. Diagrama de Flujo Procedimiento de Gestión de Incidentes de Seguridad de la Información

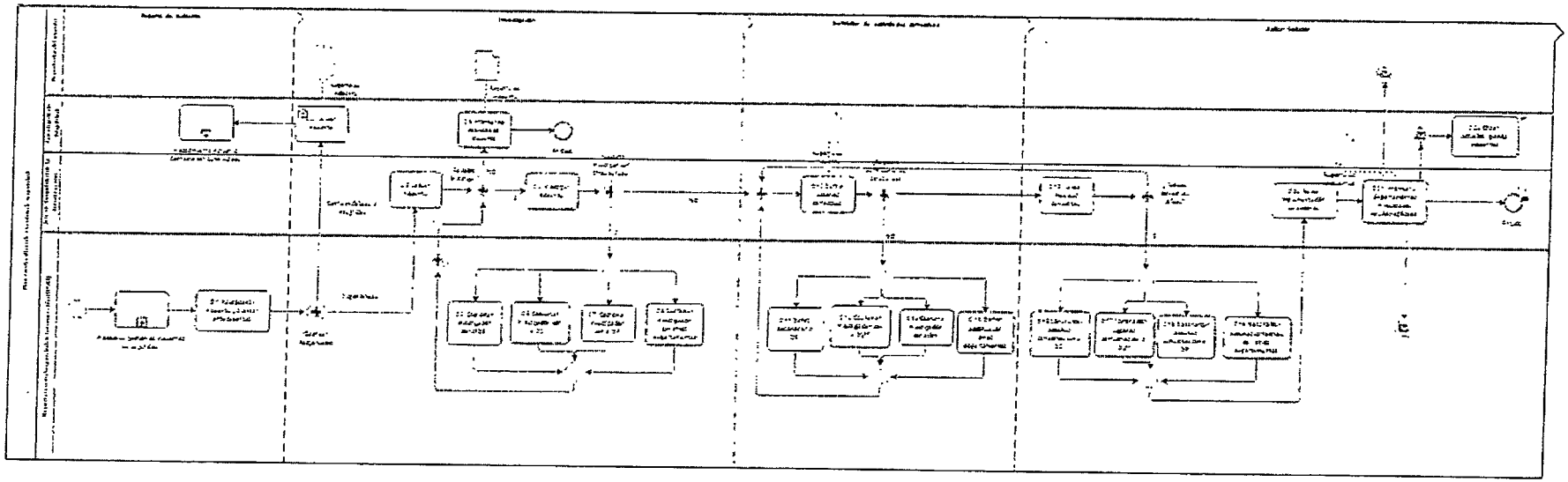

Figura 1. Procedimiento de Gestión de Incidentes de Seguridad de la Información

6.2.2 Diagrama de Flujo dividido en dos partes

6.2.2.1 Parte 1

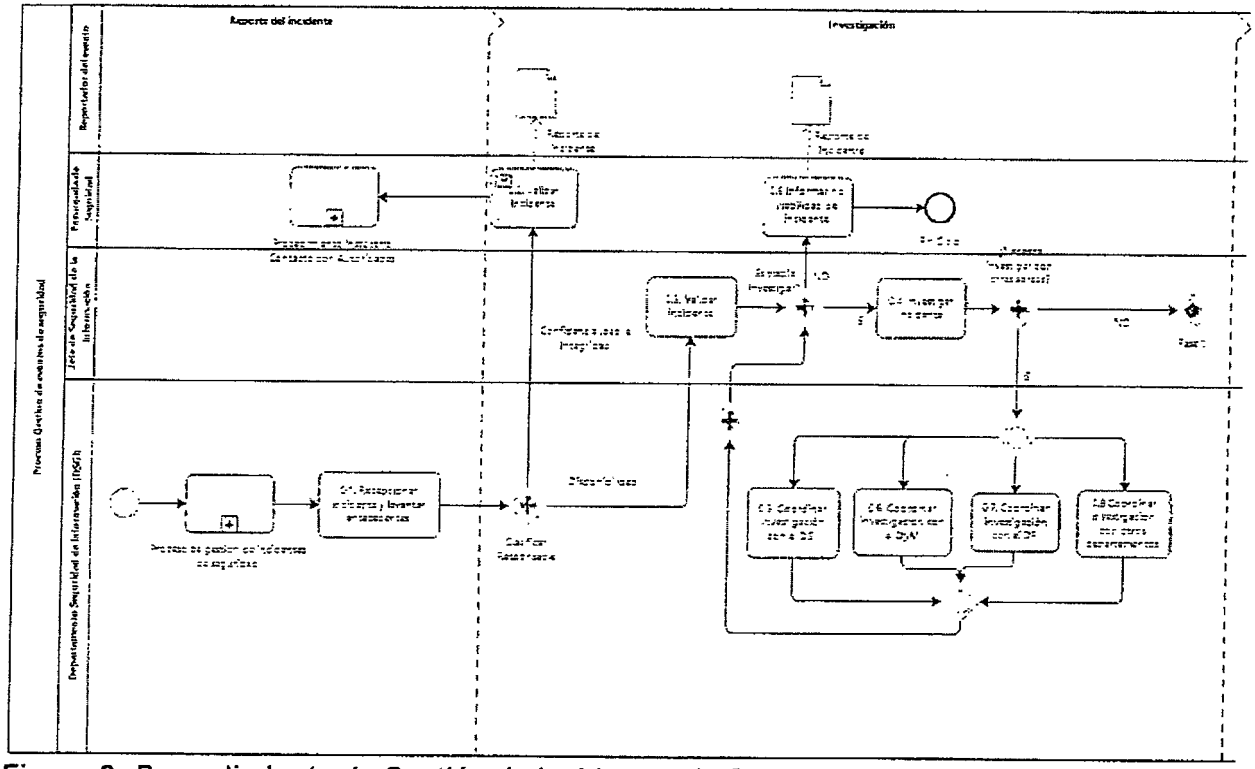

Figura 2. Procedimiento de Gestión de Incidentes de Seguridad de la Información

6.2.2.2 Parte 2

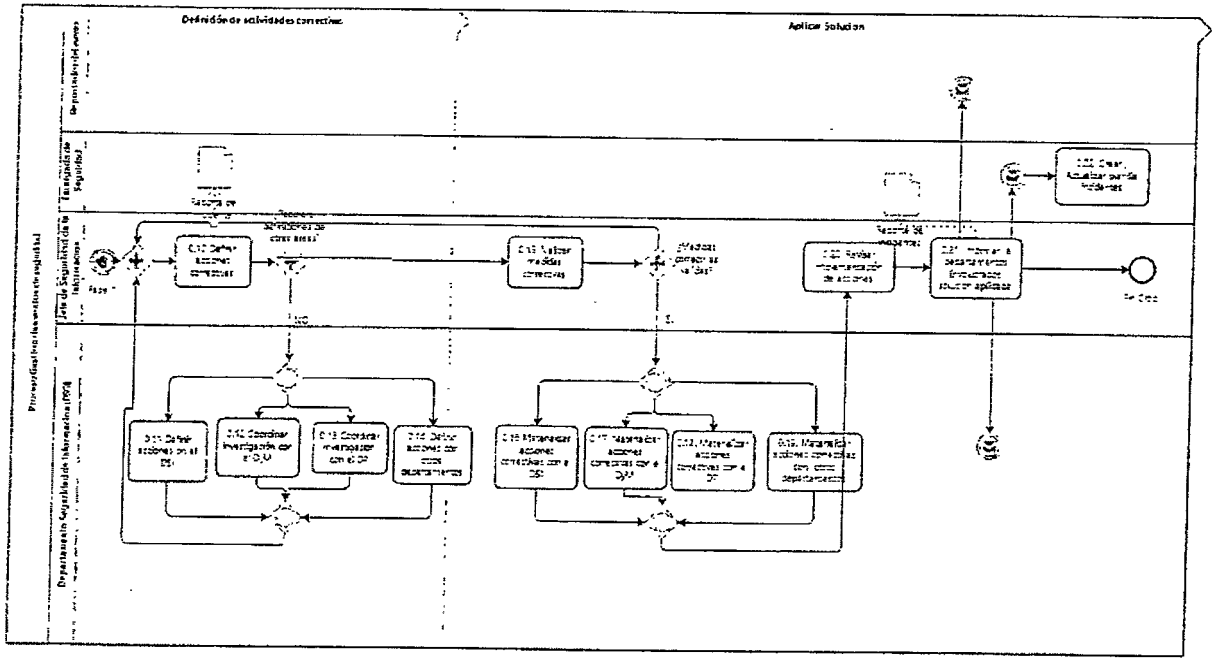

Figura 3. Procedimiento de Gestión de Incidentes de Seguridad de la Información

6.3 Matriz de Proceso

Se definen 2 tipos de casos, según el evento de seguridad que se ha detectado, en el caso de una indisponibilidad de un servicio crítico, el evento es recepcionado por el Departamento de Seguridad de la Información, en caso que el evento sea de confidencialidad o integridad, éste es recepcionado por el encargado de seguridad

El proceso se gatilla con el reporte de un incidente, que realiza un funcionario del Instituto de Prevención Social o por un incidente detectado por el proveedor del servicio, este filtro es realizado por el procedimiento de monitoreo y análisis de eventos de seguridad, una vez que sea detectado con un tipo de incidente se inician las siguientes acciones.

N°	ACTIVIDAD (Que)	RESPONSABLE (Quién)	DESCRIPCIÓN (Cómo)	Ir	SALIDA
0.1.	Recepcionar incidente y levantar antecedentes	DGSI	Se recibe la información del incidente y se levantan los antecedentes del mismo y se vinculan con las responsables según el impacto que afecte la seguridad (disponibilidad, confiabilidad e integridad)	0.2.	
0.2.	Validar Incidente	EDSI	Al detectar que el incidente afecta la confidencialidad o Integridad de los activos de información se reporta a la encargada de seguridad las características del incidente, para dar pie al procedimiento de contacto con autoridades	0.3.	Reporte Incidente / Correo Electrónico
0.3.	Validar Incidente	JDSI	Se recibe la información del incidente y los antecedentes del mismo enviados por el Jefe de Seguridad o el proveedor del servicio. En base a estos antecedentes y evaluando el impacto que tiene para los activos informáticos del Instituto de Prevención Social, valida si es un incidente para investigar o no, en el caso que proceda pasa a actividad N° 0.4, si no pasa actividad N° 0.8 y envía correo electrónico a la ESDI, dando la razón por la cual no se realizara la investigación asociada al incidente.	0.4.	Correo Electrónico

N°	ACTIVIDAD (Que)	RESPONSABLE (Quién)	DESCRIPCIÓN (Cómo)	Ir	SALIDA
0.4.	Investigar incidente	JDSI	Se procede a investigar las causas, ámbitos afectados, nivel de daño causado, etc. con todas las áreas pertinentes al incidente producido. Si es necesario investigar en otra área o departamento pasa a actividad 0.6, sino pasa a actividad 0.6, 0.7 o 0.8 según sea el caso.	0.5.	
0.5.	Coordinar investigación con el DSGI	DSI	En particular se investiga en coordinación con el DSGI, revisando los registros del monitoreo a la operación de los servicios.	0.6.	Registros Monitoreo
0.6.	Coordinar investigación con DyM	DyM	En particular se investiga en coordinación con el área de Desarrollo, revisando los registros del monitoreo a las aplicaciones del servicio.	0.7.	Registros Monitoreo
0.7.	Coordinar investigación con DP	DP	En particular se investiga en coordinación con el área de Operaciones, revisando los registros del monitoreo a las aplicaciones del servicio.	0.8	Registros Monitoreo
0.8	Coordinar investigación con otra Área o departamento	DSI	En particular se investiga en coordinación con otros departamentos, revisando los registros del monitoreo a las aplicaciones del servicio.	0.9.	Registros Monitoreo
	¿Necesita investigar con otras Áreas?	DP	¿Necesita investigar con otras Áreas? Si no es necesario continuar investigando con otras áreas, continúa con la actividad 0.6, 0.7 o 0.8 según corresponda. En caso contrario vuelve a un nuevo ciclo de coordinación para continuar con la investigación.		

N°	ACTIVIDAD (Que)	RESPONSABLE (Quién)	DESCRIPCIÓN (Cómo)	Ir	SALIDA
0.9.	Informar no viabilidad	EDSI	Informa vía correo electrónico el reporte de incidente al Jefe de Seguridad de la información, que el incidente no genera impacto sobre los activos de información de la organización	0.11	Reporte Incidente / Correo Electrónico
0.10	Definir acciones correctivas	JDSI	Con todos los antecedentes del problema y el análisis producto de la investigación efectuada, se completa el reporte de incidente, se definen las acciones correctivas en coordinación con las áreas pertinentes al incidente producido.	0.11	Reporte Incidente / Correo Electrónico
	¿Requiere definición de otra área departamento?		La Encargada de Seguridad de la Información define si hay otra área o departamento de la institución no informáticas, que deben participa en las acciones correctivas determinadas por el Jefe de Seguridad.		Correo electrónico
0.11	Definir acciones con el DSGI	DSI	En particular se definen las acciones correctivas en coordinación con el DSGI por ejemplo, si ciertas IP están atacando o son demasiado recurrentes o que van apuntando a algún servidor interno en particular, entonces se averigua y se indaga cuáles son esas IP, para eventualmente bloquearlas	0.12	
0.12	Coordinar investigación con DyM	DyM	En particular se definen las acciones correctivas en coordinación con el área de Desarrollo, por ejemplo, si ciertas máquinas atacadas tienen alguna vulnerabilidad que se puede remediar modificando el código de las mismas que dé solución a una vulnerabilidad.	0.13	
0.13	Coordinar investigación con DP	DP	En particular se definen las acciones correctivas en coordinación con el área de Desarrollo, por ejemplo, si ciertas máquinas atacadas tienen alguna vulnerabilidad que se puede remediar usando algún parche	0.14	
0.14	Definir acciones con otras áreas	DSI	Eventualmente, si el incidente lo amerita, se coordinan acciones correctivas con otras áreas. Las mismas que participaron en la investigación, o nuevas áreas.		

N°	ACTIVIDAD (Que)	RESPONSABLE (Quién)	DESCRIPCIÓN (Cómo)	Ir	SALIDA
0.15	Validar medidas correctivas	EDSI	El Jefe de Seguridad de Información recibe las medidas tomadas por el DSGI y las áreas que han definido la formulación de la solución de la problemática causada por la incidencia de seguridad detectada, el análisis debe demostrar que las áreas han realizado un análisis de causa raíz.	0.16	Correo electrónico
	Medidas Correctivas Válidas		El ESI valida las medidas pasar según corresponda a 0.16, 0.17, 0.18 y 0.19 ; sino las valida, volver a 0.10		
0.16	Materializar acciones correctivas con DSGI	DSI	El DSGI materializa las acciones correctivas a través de los proveedores externos que administran la plataforma tecnológica, por ejemplo, para aplicar parches de seguridad, bloquear el dominio que originó el incidente, etc.	0.17	Correo electrónico
0.17	Materializar acciones correctivas con DyM	DyM	El DyM materializa las acciones correctivas a través de los proveedores externos que administran la plataforma tecnológica, por ejemplo, para aplicar parches de seguridad, bloquear el dominio que originó el incidente, etc.	0.18	Correo electrónico
0.18	Materializar acciones correctivas con DP	DP	El DDO materializa las acciones correctivas a través de los proveedores externos que administran la plataforma tecnológica, por ejemplo, para aplicar parches de seguridad, bloquear el dominio que originó el incidente, etc.	0.19	Correo electrónico

N°	ACTIVIDAD (Que)	RESPONSABLE (Quién)	DESCRIPCIÓN (Cómo)	Ir	SALIDA
0.19	Materializar acciones correctivas otras Aéreas	DSI	El DSGI deben materializar las acciones especificadas con respecto al incidente levantando. A través de la Sección de Comunicaciones, se informará del incidente a todo el personal, las soluciones aplicadas y se difunden buenas prácticas que eviten su repetición en el futuro.	0.20	
0.20	Revisar Implementación de acciones	JDSI	El JDSII debe revisar las acciones tomadas por las distintas áreas de la Institución y validar que se ha solucionado el incidente generado , material de respaldo (Reporte Incidente / Correo Electrónico)	0.21	Reporte Incidente / Correo Electrónico
0.21	Informar a departamentos Involucrados	JDSI	Se le informa a los departamentos involucrados y a la EDSI vía correo la solución del incidente	0.22	Correo Electrónico
0.22	Crear / Actualizar planilla de incidentes	EDSI	Crear / Actualizar planilla de registro de incidentes	Fin Ciclo	

7. INDICADORES DE GESTION

Nombre del indicador	Formula	Clasificación del Resultado o Criterio de Aplicación			Seguimiento	Cumplimiento	Registros (medios de verificación)
		Muy Satisfactorio	Satisfactorio	Insatisfactorio			
Porcentaje de Incidentes de seguridad reportados y resueltos en el año.	N° de incidentes de seguridad resueltos en el año t / N° Total de incidentes de seguridad reportados en el año t) * 100	> 90% y ≤ 100%	> 50% y ≤ 80%	≤ 50%	Mensual	Diciembre	- Informe de incidentes de seguridad.

8. CONTROL DE REGISTROS

Nombre del Registro	Tipo	Responsable	Ubicación	Soporte	Medio de Almacenamiento (Recuperación)	Tiempo de Retención	Disposición
Formulario incidente de seguridad	Documento	Departamento Seguridad de Información (DSI	//DSI/SeguridadIncidentes	Digital	Carpeta digital Incidentes Seguridad	6 años	No aplica
Planilla Incidentes	Documento	Encargada Seguridad de la Información (EDSI)	//DSI/SeguridadIncidentes	Digital	Carpeta digital Incidentes Seguridad	6 años	No aplica
Correo Electrónico Eventos	Correo Electrónico	Departamento Seguridad de Información (DSI)	Carpeta Digital Incidentes Correo electrónico	Digital	Carpeta Digital Incidentes Correo electrónico	6 años	No aplica
Registros Monitoreo	Correo Electrónico	Departamento Seguridad de Información (DSI)	Carpeta Digital Incidentes Correo electrónico	Digital	Carpeta Digital Incidentes Correo electrónico	6 años	No aplica

	PROCEDIMIENTO DE GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			DIVISION DE INFORMATICA
	Nivel de Confidencialidad	Uso Interno	Versión	01
			Fecha de Aprobación Legal	08 JUN 2016
			Página	28 de 29

9. ANEXOS

A.1 Formulario Incidentes de Seguridad

	FORMULARIO INCIDENTE DE SEGURIDAD			SUBDIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS
	Nivel de Confidencialidad	Uso Interno	Número de Registro	XXXXX0000
			Fecha y Hora	DD.MM.2016 / HH:MM
			Responsable	Encargada de Seguridad de la Información

INFORMACION INCIDENTE			
Tipo de Incidente		Sistema	
Descripción Incidente			
Usuarios Afectados			
Administrador Proyecto			
Causa de la Caida			
Minutos | Horas | Días			
Observaciones del Caso			
Procedimiento realizado			

FIRMA ENCARGADA DE SEGURIDAD DE LA INFORMACIÓN

FIRMA SUBDIRECTORA DE ADMINISTRACIÓN Y FINANZAS

A.2 Planilla de Incidentes

PLANILLA INCIDENTES DE SEGURIDAD DEL INSTITUTO DE PREVISION SOCIAL (IPS)

INFORME INCIDENTE DE SEGURIDAD NUMERO *XXXXXNMAA* *RESPONSABLE Encargada de Seguridad de la Información*

MES / _____ AÑO/ _____

REGISTRO INCIDENTE			DURACION CAIDA			DETALLE INCIDENTE		
N°	FECHA	SISTEMA	MINUTOS	HORAS	DIAS	N° USUARIOS AFECTADOS	ADMINISTRADOR PROYECTO	CAUSA DE LA CAIDA

OBSERVACIONES