SE APRUEBA PARA EL INSTITUTO DE PREVISIÓN SOCIAL, EL DOCUMENTO DENOMINADO "PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN" Y DEJA SIN EFECTO RESOLUCIÓN EXENTA N° 528, DE 02.11.2017, DICTADA SOBRE IGUAL MATERIA.

RESOLUCIÓN EXENTA Nº 430

SANTIAGO, 13 NOV 2018

V I S T O S:

1.- La Ley Nº 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. Nº 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.- La Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, cuyo texto refundido, coordinado y sistematizado se encuentra establecido en el D.F.L. N° 1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia.

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. Nº 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 Nº 20.255.

C O N S I D E R A N D O:

1.- Que, por Resolución Exenta N° 528, de 02 de noviembre de 2017, esta Dirección Nacional aprobó el "Procedimiento Gestión de Incidentes de Seguridad de la Información", con aprobación legal de fecha 11 de octubre de 2017.

2.- Que, para efectos de asegurar una consistente y eficaz gestión de los incidentes de seguridad de la información y de los mecanismos iniciales de respuesta, generando una metodología común para la investigación, evaluación, respuesta, recolección de evidencias y acciones de mitigación, incluida la comunicación sobre eventos de seguridad y debilidades, el Departamento de Gestión de Riesgos de Sistemas de Información de la División Informática de este Instituto, ha actualizado el procedimiento referido en el Considerando precedente, cuyo texto fue revisado por el Encargado de Seguridad de la Información y aprobado por el Presidente del Comité de Seguridad de la Información.

3.- Que, por Oficio Ordinario Nº 48516/2164-18, de 25 de octubre de 2018, la División Jurídica de este Instituto, emitió informe sobre la aprobación legal del procedimiento de la especie, estableciendo la procedencia de dictar la correspondiente resolución aprobatoria por el Departamento Secretaría General y Transparencia, la que por su naturaleza se encuentra exenta del trámite de toma de razón, por la Contraloría General de la República.

R E S U E L V O:

1.- Apruébase para el Instituto de Previsión Social, el "Procedimiento Gestión de Incidentes de Seguridad de la Información", que consta de veinticuatro (24) páginas, que se adjunta como parte integrante de la presente Resolución Exenta, aprobado por la División Jurídica con fecha 25 de octubre de 2018, cuyo objetivo es asegurar una consistente y eficaz gestión de los incidentes de seguridad de la información y de los mecanismos iniciales de respuesta, generando una metodología común para la investigación, evaluación, respuesta, recolección de evidencias y acciones de mitigación, incluida la comunicación sobre eventos de seguridad y debilidades.

2.- Publíquese el procedimiento, que se aprueba por el presente acto administrativo, en el ambiente "Procedimientos 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 3 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.

4.- Déjase sin efecto, a contar de la total tramitación del presente Instrumento, la Resolución Exenta N° 528, de 02 de noviembre de 2017, dictada sobre la misma materia.

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

PATRICIO CORONADO ROJO
DIRECTOR NACIONAL
INSTITUTO DE PREVISIÓN SOCIAL

DISTRIBUCION:

- Gabinete Dirección Nacional
- Subdirección de Servicios al Cliente
- Subdirección de Sistemas de Información y de Administración
- División Jurídica
- División Beneficios
- División Canales de Atención al Cliente
- División Planificación y Desarrollo
- División Informática
- Departamento Contraloría Interna
- Departamento Gestión y Desarrollo de Personas
- Departamento Administración e Inmobiliaria
- Departamento Cobranza Institucional
- Departamento Secretaría General y Transparencia
- A los Directores Regionales IPS, quienes deberán comunicar el presente instrumento a los CAPRI de su dependencia
- Unidad Apoyo Documental de la División Jurídica

YGF/ASO/JRAB/BAC/RPY/rpy
"Procedimiento Gestión de Incidentes de Seguridad de la Información".
X- 84 (Folio D.S.G.T. 3575-175-1)

PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Elaborado por:	Revisado por:	Aprobado por:
Jefe Departamento de Gestión de Riesgos de Sistemas de Información.	Encargado de Seguridad de la Información	Presidente Comité de Seguridad de la Información. Jefe División Jurídica. Director Nacional.

INSTITUTO DE PREVISIÓN SOCIAL VºBº DPTO. CONTROL JURIDICO

CONTROL DE CAMBIOS

Fecha	Versión	Página	Numeración del contenido	Cambio Efectuado/Nombre del responsable
08/06/2016	01	Todas	Todas	**Jefe DSI**/Versión inicial del Documento Aprobado Resolución Exenta N°316 de 01.07.2016
11.10.2017	02	4,5,6	2,3,4,7	**Jefe DSI**, Actualización la redacción de alcance, documentos de referencia y definiciones, se indica responsabilidad por mantener indicador. Aprobado Resolución Exenta N°528 de 02.11.2017
	03			(Cambios propuestos 2018)

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 con 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).

NOTA DE ACLARACIÓN

En virtud de lo dispuesto en la Resolución Exenta N°644 de 22 de diciembre del 2017, del Instituto de Previsión Social, sobre Estructura Orgánica, Objetivos y Funciones del IPS, numeral 5, se entienden derogadas expresamente las Resoluciones Exentas N°320 de 19 de julio de 2012; Resolución Exenta N°231 de 24 de febrero de 2014; Resolución Exenta N°610 de 9 de noviembre de 2015, todas de este Instituto, por tanto el Departamento de Seguridad de Información, se denomina a partir del 22 de diciembre 2017, Departamento Gestión de Riesgos de Sistemas de Información.

TABLA DE CONTENIDOS

1. OBJETIVO 4

2. ALCANCE 4

3. DOCUMENTOS DE REFERENCIA 5

4. DEFINICIONES, SIGLAS Y TERMINOS. 6

5. ROLES Y RESPONSABILIDADES 8

6. DESCRIPCIÓN DEL PROCEDIMIENTO 10

6.1 Descripción de Actividades 10

6.2 Diagrama de Flujo 14

6.3 Matriz de Proceso 17

7. INDICADORES DE GESTIÓN 19

8. CONTROL DE REGISTROS DE OPERACIÓN 19

9. ANEXOS 20

Anexo 1 Formulario de Incidente de Seguridad 20

Anexo 2 Planilla Incidentes 23

Anexo 3 Guía de evaluación de la criticidad 24

1. OBJETIVO

Asegurar una consistente y eficaz gestión de los incidentes de seguridad de la información, los mecanismos iniciales de respuesta, generando una metodología común para la investigación, evaluación, respuesta, recolección de evidencias y acciones de mitigación, incluida la comunicación sobre eventos de seguridad y debilidades.

2. ALCANCE

Este procedimiento general, debe ser aplicado como guía para el desarrollo de los diferentes procedimientos de respuesta a incidentes.
El procedimiento aplica a todos quienes cumplen funciones para el Instituto de Previsión Social (IPS), sea esto en sus instalaciones o fuera de ellas, aplicándose a funcionarios de cualquier estamento y calidad jurídica (planta, contrata, honorarios, asesores, consultores, alumnos en práctica) así como también a personas naturales y jurídicas externas, públicas o privadas que presten servicios en el Instituto o para este y que tengan participación en las actividades descritas en este documento.

El foco de este procedimiento se sustenta en el Dominio 16 de la norma Nch-ISO 27001:2013 referido a la Gestión de Incidentes de Seguridad de la Información y mejoras, considerando las responsabilidades institucionales, la obligación de informar los incidentes, su evaluación y respuesta, la recolección de evidencias, análisis forense si se estima necesario, el correspondiente aprendizaje y mejoras de las fragilidades identificadas.

El ámbito de ejecución del procedimiento son todos los activos de información del IPS y aquellos bajo su responsabilidad que estén señalados en el documento. Su cobertura se extiende a la información impresa y también a aquella almacenada electrónicamente, y transmitida por cualquier soporte o medio. Se debe precisar que el presente alcance descrito en los párrafos anteriores está circunscrito y detallado en el documento "SGSI-00 ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)".

3. DOCUMENTOS DE REFERENCIA

a) Resolución Exenta N° 175, del 28.03.2017, Política General de Seguridad de la Información del IPS, de la Dirección Nacional.

b) Resolución Exenta N° 292 del 21.06.2017, Documento Alcance del Sistema de Gestión de la Seguridad de la Información, de la Dirección Nacional.

c) Resolución Exenta N° 385 del 10.08.2017, Política Organización de la Seguridad de la Información, de la Dirección Nacional.

d) Resolución Exenta N° 479, de 04.10.2017, Procedimiento de Monitoreo y Análisis de Eventos de Seguridad, de la Dirección Nacional.

e) Resolución Exenta N° 528, de 09.11.2017, Política de Gestión de Incidentes de Seguridad de la información, de la Dirección Nacional.

f) Resolución Exenta N° 644, de 22.12.2017, que aprueba Estructura Orgánica del Instituto de Previsión Social, de la Dirección Nacional.

g) Resolución Exenta N° 55, de 09.02.2018, Procedimiento de Contacto con Autoridades, de la Dirección Nacional.

h) Resolución Exenta N°361 del 27.08.2018, de la Dirección Nacional, que modifica las Resoluciones Exentas que integran el Sistema de Gestión de Seguridad de la Información del IPS que se señalan en los numerales 8 y 10, según indica.

i) Norma NCh-ISO 27001:2013, Sistemas de Gestión de la Seguridad de la Información – Requisitos.

INSTITUTO DE PREVISIÓN SOCIAL V°B° DEPTO. CONTROL JURÍDICO

4. DEFINICIONES, SIGLAS Y TERMINOS.

Definiciones utilizadas en procedimiento

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

b. **Áreas Operativas:** Son departamentos que resguardan, mantienen y mejoran la integridad, confiabilidad y disponibilidad de los servicios del negocio. Está compuesto por las jefaturas de los siguientes departamentos: Departamento de Desarrollo y Mantención de Sistemas, Departamento de Tecnología, Departamento de Producción y Departamento de Gestión de Riesgos de Sistemas de Información; además del Jefe División Informática del IPS y de la Encargada de Seguridad de la Información.

c. **Base de conocimiento:** Tipo especial de base de datos para la gestión del conocimiento.

d. **Debilidad:** Deficiencia de uno o de un grupo de activos, los que pueden ser explotados por amenazas que ponen en riesgo la confidencialidad, integridad y disponibilidad de los mismos.

e. **Evento:** Incidente y/o ocurrencia identificada en el estado de un sistema, servicio o red, indicando una posible violación de la seguridad de la información, política o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

f. **Gestión de eventos e información de seguridad (SIEM, por su sigla en inglés):** Herramienta Tecnológica de correlación de logs y análisis de eventos.

Definiciones generales

a. **Activo de Información:** Elementos para la producción, procesamiento, emisión, almacenaje, comunicación, visualización y la recuperación de la información que posee valor para la organización. Pueden clasificarse en personas, infraestructura, sistemas y datos.

b. **Buen uso de la información:** Cuidado que los colaboradores de la Institución deben procurar en el manejo o utilización de los sistemas y activos de información de la Institución, refiérase al cuidado que los usuarios deben tener en relación a los activos de información.

c. **Confidencialidad**: Propiedad de la información que consiste en que ésta no sea puesta a disposición o sea revelada a individuos, entidades o procesos no autorizados.

d. **Continuidad del negocio:** Es la mantención de las actividades propias del instituto a pesar la ocurrencia de eventos que la pongan en peligro, lo que se logra por el establecimiento de medidas que mitiguen las interrupciones de las actividades, asegurando la disponibilidad e integridad de los activos de información, o minimizando la pérdida de datos relevantes para el proceso.

e. **Custodio de la información:** Funcionario que mantiene bajo su responsabilidad, información de la que no es propietario, pero que, por su función es el responsable de aplicar las medidas de seguridad necesarias, de acuerdo al valor de los activos a su cargo. Son individuos o grupos que proveen un alto nivel de confianza y a los cuales se les deja en posesión y responsabilidad, delegada por su dueño, de velar por la seguridad de información que no les pertenece. Este rol es ejecutado, normalmente, por personal de Informática, para la información digital. Entre sus deberes están los respaldos y sus verificaciones, la recuperación de información desde dichos respaldos y mantener los registros con los resguardos asociados a su nivel de clasificación. Los custodios de información física son responsables de protegerla y resguardarla de accesos indebidos o no autorizados.

f. **Documento electrónico:** Toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.

g. **Disponibilidad:** Propiedad de la información que consiste en que ésta deba estar accesible y utilizable cuando lo requiera una entidad autorizada.

h. **Evento de Seguridad de la Información:** Acontecimiento que amenaza la seguridad de la información, sin presentar resultados negativos.

i. **Jefatura:** Funcionario encargado de un grupo de personas, conformados en, dirección, subdirección, división, departamento o área que lo amerite definida en la estructura organizativa del instituto.

j. **Incidente de seguridad de la información**: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

k. **Integridad:** La propiedad de proteger la exactitud y completitud de los activos

INSTITUTO DE PREVISION SOCIAL V°B° DEPTO CONTROL JURIDICO

l. **Plan de Continuidad:** Es un plan de emergencia con el objetivo de mantener la funcionalidad de la organización a un nivel mínimo aceptable durante una contingencia.

m. **Plan de Cuentas:** Relación que existe entre los usuarios, roles y perfiles definidos en la institución considerando las condiciones incompatibles en cada uno de ellos.

n. **Propietario de la información:** Es quien genera, mantiene y utiliza la información, siendo responsable de ella y de los procesos que se llevan a cabo en su procesamiento, a través de diversos medios, sean éstos manuales, mecánicos o electrónicos.

o. **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.

p. **Tercero:** Empresa o persona externa que tiene algún tipo de relación con la Institución.

5. ROLES Y RESPONSABILIDADES

a) **Encargado de Seguridad de la Información (ESI):** Es el funcionario que supervisa el cumplimiento de las políticas de seguridad de la información, establece nexo con sus pares en la materia que pertenezcan a otros servicios, y comunica incidentes de seguridad a la Alta Dirección. Dirige y preside el Comité de Seguridad de la Información.

b) **Jefe Departamento Gestión de Riesgos de Sistemas de Información (Jefe DGRSI):** Es el encargado de gestionar y controlar el sistema de seguridad de la información, como también los activos de información del instituto, conforme a la normativa vigente y los objetivos estratégicos institucionales. Es el responsable de informar al Comité de Seguridad de la Información y al Encargado de Seguridad de la Información, con respecto a la evaluación del daño provocado por un incidente de seguridad de la información y mantener información del indicador.

c) **Jefes de Departamentos de la División Informática (Áreas operativas):** Responsables de asegurar la continuidad operativa de los diferentes equipamientos y/o servicios informatizados del IPS, gestionando las actividades necesarias con el área resolutora específica según el tipo de incidentes y el escalamiento a los niveles que correspondan, de ser necesario, a objeto de dar solución a los incidentes o requerimientos presentados.

d) **Funcionarios de IPS:** Responsables de cumplir con lo establecido en el presente instrumento y aplicarlo en su entorno laboral. Tiene la obligación de alertar de manera oportuna y adecuada por los canales y procedimientos formalmente establecidos, cualquier situación que pueda poner en riesgo la seguridad de la información.

e) **Mesa de Ayuda Técnica:** Responsable de recibir reporte, investigar, clasificar los eventos reportados según el departamento, unidad o área relacionado e informar los eventos potenciales categorizados como incidentes al Jefe Departamento Gestión de Riesgos de Sistemas de Información para su investigación y/o solución según corresponda.

INSTITUTO DE PREVISION SOCIAL V°B° DEPTO CONTROL JURIDICO

6. DESCRIPCIÓN DEL PROCEDIMIENTO

6.1 Descripción de Actividades

Los incidentes se pueden originar y materializar de diferentes maneras. Por tanto, este procedimiento se enfoca a una forma general de resolverlos, buscando minimizar el riesgo para la Institución.

En este contexto, el Jefe del Departamento Gestión de Riesgos de Sistemas de Información, en forma mensual informará al Encargado de Seguridad de Información (ESI) de todos los incidentes ocurridos durante el período (mes a evaluar), a través de una planilla de incidentes que se genera con la periodicidad anterior (mes a mes) (Ver Anexo 2).

6.1.1 Notificación y validación del Incidente.

Existen dos (2) formas de notificación de incidentes de seguridad de la información, los cuales se encuentran descritos en el **"Procedimiento de monitoreo y análisis eventos de seguridad"** los que se detallan:

- Incidentes reportados por funcionarios de IPS a través de la mesa de ayuda por medio de ticket.
- Incidentes reportados por el sistema de monitoreo de servicios del SOC por correo electrónico.

El Jefe del Departamento Gestión de Riesgos de Sistemas de Información validará lo reportado y definirá la clasificación correspondiente, según la criticidad evaluada (Ver Anexo 3) para el activo de información.

- Al validar el incidente de seguridad, el Jefe del Departamento Gestión de Riesgos de Sistemas de Información inicia el tratamiento del incidente utilizando el **"Formulario de Incidentes de Seguridad".** (Ver Anexo 1)

- Al reclasificar el incidente como un evento, vuelve al "Procedimiento de monitoreo y análisis eventos de seguridad", vía correo electrónico al Departamento de Gestión de Riesgos de Sistemas de Información para dar solución.

En el "**Formulario de Incidentes de Seguridad"** (Ver Anexo 1) se clasificará los tipos de incidentes siguiendo la triada de seguridad de la información. Los incidentes pueden clasificarse en más de un tipo (Ver tabla 1), dependiendo de los activos de información involucrados.

Tabla 1.

Clasificación

Confidencialidad	a) Fuga de Información b) Acceso físico no autorizado c) Acceso no autorizado a los sistemas de información d) Código malicioso e) Filtración de información reservada
Integridad	a) Corrupción de datos b) Incidentes provocados por la naturaleza
Disponibilidad	a) Indisponibilidad del servicio b) Denegación de servicios computacionales c) Fallas del sistema información

El Jefe del Departamento Gestión de Riesgos de Sistemas de Información aplicará los niveles de prioridad (Ver tabla 2), que permiten determinar los recursos para buscar la solución del incidente. La priorización se basa esencialmente en los siguientes parámetros

Tabla 2

Parámetro	Descripción	Variables
Criticidad	Importancia del incidente dependiendo de los procesos y de usuarios afectados.	**Alto:** Interrumpe seriamente los procesos de la Institución, afecta a más de cinco funcionarios. **Medio**: Interrumpe momentáneamente los procesos de la Institución y afecta a más de un funcionario, pero menos de cinco. **Bajo:** No interrumpe los procesos generales de la Institución y afecta solo a un usuario.

El Jefe del Departamento Gestión de Riesgos de Sistemas de Información debe contactar a quien reportó el incidente para recolectar todos los antecedentes en el **"Formulario de Incidentes de Seguridad"** (Ver Anexo 1).

Los antecedentes son:

- Identificación de quien reporta
- Que originó el incidente.
- Fecha reporte
- Hora reporte
- Activos / Sistemas afectados
- Descripción

Luego, envía los antecedentes del formulario al Encargado de Seguridad de la Información (ESI).

El Encargado de Seguridad de la Información (ESI) recepciona los antecedentes del incidente e inicia el **"Procedimiento de Contacto con Autoridades"**.

6.1.2 Tratamiento del Incidente

El Jefe del Departamento Gestión de Riesgos de Sistemas de Información, en coordinación con las jefaturas de las áreas operativas, realiza una investigación para desarrollar la solución del incidente, registrando todos los antecedentes en el "**Formulario de Incidentes de Seguridad"** (Ver Anexo 1).

Los antecedentes son:

- Responsable de la acción inmediata
- Acción inmediata realizada
- Fecha acción inmediata
- Descripción

De ser necesario, el Jefe del Departamento Gestión de Riesgos de Sistemas de Información podría definir la necesidad de un análisis forense especializado, el que será planificado y gestionado según el tipo y criticidad del incidente particular, entregando la información pertinente al área designada o entidad externa, según se defina caso a caso.

6.1.3 Tratamiento del incidente no resuelto

Si el incidente no se ha podido resolver, el Jefe del Departamento Gestión de Riesgos de Sistemas de Información, en coordinación con el Jefe de la División Informática, citará a una reunión de trabajo a los jefes de los siguientes Departamentos (o quienes los Subroguen).

- Departamento de Tecnología
- Departamento de Producción
- Departamento de Desarrollo y Mantención de Sistemas

Quienes vuelven a iniciar el ciclo de investigación para desarrollar en conjunto la solución del incidente como prioridad máxima dentro de sus funciones. Esta actividad debe ser realizada todas las veces que sea necesario, hasta mitigar el incidente.

6.1.4 Recolección de evidencias.

Durante todo el proceso de respuesta, análisis forense de ser necesario, y mitigación, se deben recolectar las evidencias necesarias de las acciones y cambios realizados, por el área operativa específica designada según el tipo de incidente, las que podrán ser de utilidad para procesos de análisis posterior. Estas evidencias, deben ser entregadas al Departamento de Gestión de

Riesgos de Sistemas de Información y resguardadas por éste con el objetivo de protegerlas de alteraciones o borrado.

6.1.5 Cierre del Incidente

Una vez mitigado o solucionado el incidente, el Jefe del Departamento Gestión de Riesgos de Sistemas de Información, actualiza los antecedentes del formulario asegurándose que todos los campos del formulario estén completos. Los antecedentes son:

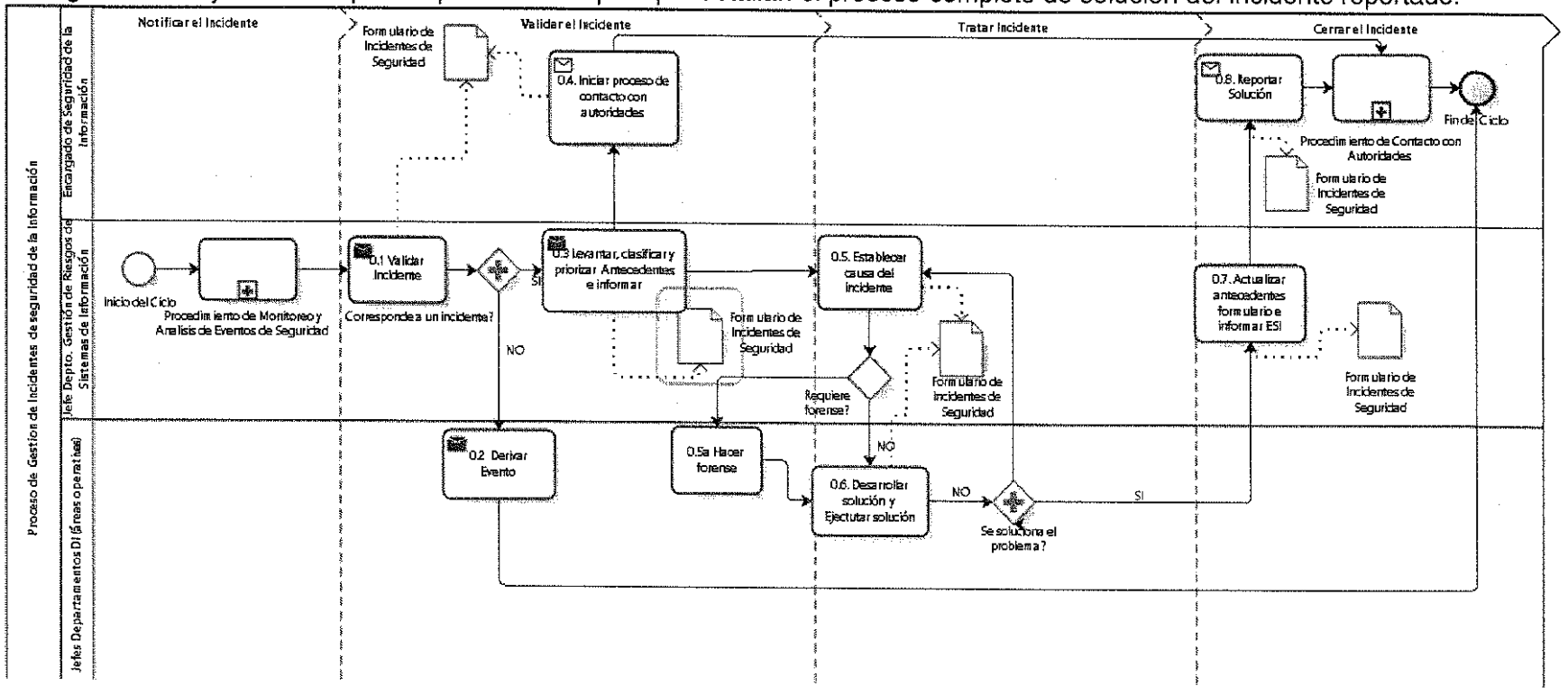
- Análisis de Causas
- Costos Asociados
- Acción Correctiva/ Preventiva
- Fecha Cierre
- Descripción

Terminado de completar los campos del **"Formulario de Incidentes de Seguridad"** (Ver Anexo 1), el Jefe del Departamento Gestión de Riesgos de Sistemas de Información, envía al Encargado de Seguridad de la Información el formulario completo, quien recepciona los antecedentes y continúa con el **Procedimiento de contacto con autoridades**.

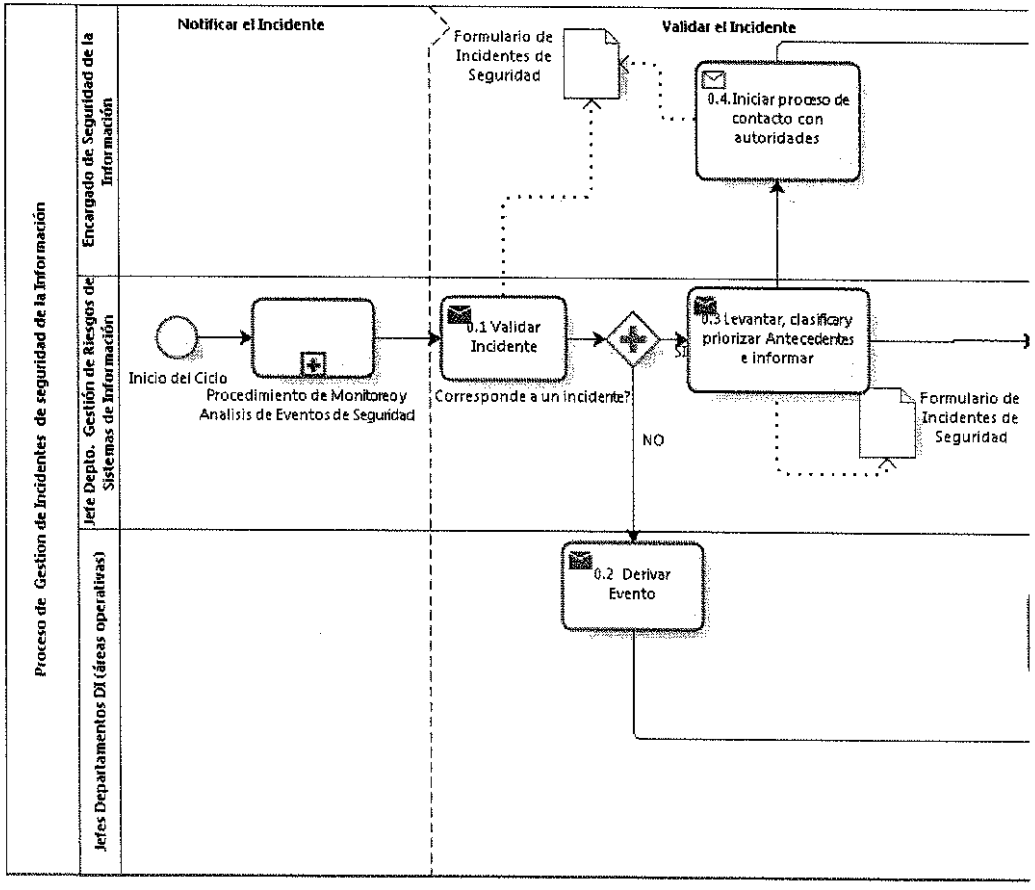
6.2 Diagrama de Flujo

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

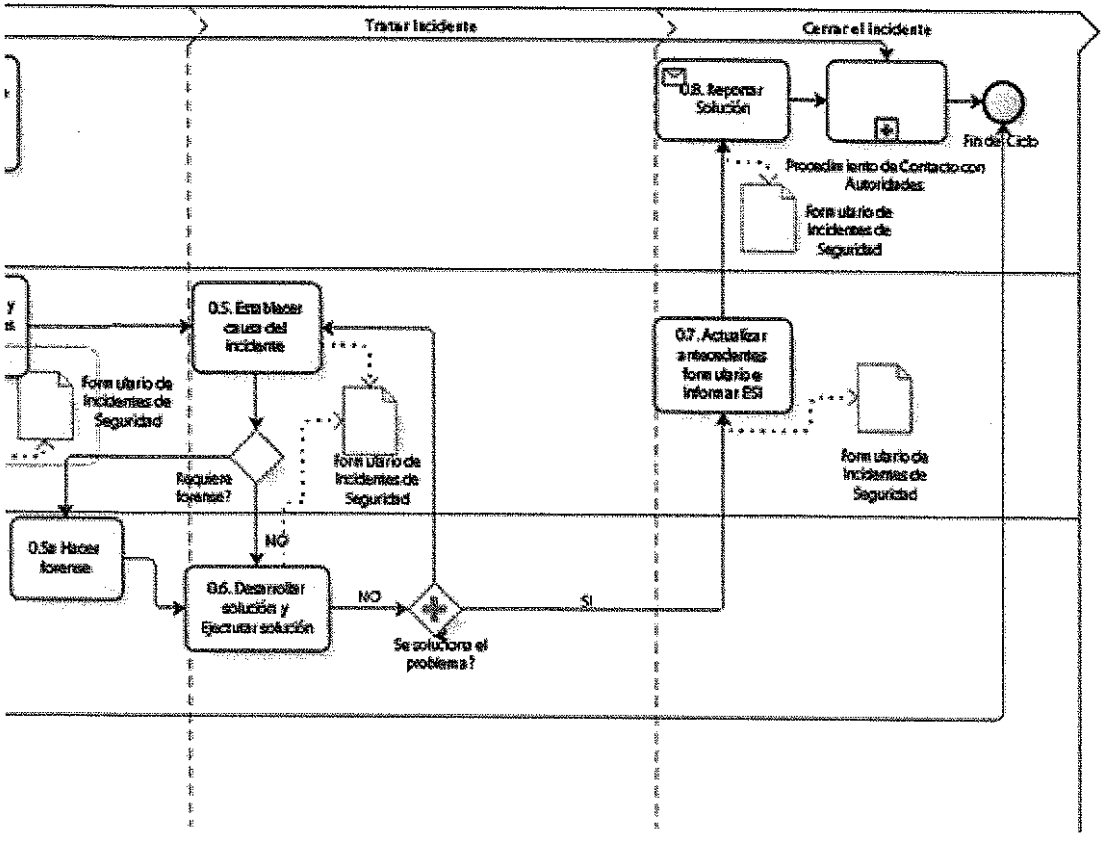
El diagrama de flujo está compuesto por varias etapas que detallan el proceso completo de solución del incidente reportado.



6.2.2 Notificar y validar el Incidente



6.2.3 Tratar y Cerrar el incidente



Este documento impreso es una copia no controlada

6.3 Matriz de Proceso

N°	ACTIVIDAD (Que)	RESPONSABLE (Quién)	DESCRIPCIÓN (Cómo)	Ir	SALIDA
0.1	Validar Incidente	Jefe del Departamento Gestión de Riesgos de Sistemas de Información	Valida con los datos recopilados si corresponde a un incidente o debe ser tratado como evento. Si corresponde a evento se debe continuar con la actividad 0.2. Si corresponde a Incidente se debe continuar con la actividad 0.3.	0.2 0.3	Incidente validado en el Formulario de Incidente de Seguridad o correo electrónico para solucionar evento
0.2	Derivar Evento	Jefe del Departamento Gestión de Riesgos de Sistemas de Información	De ser considerado un evento, se gestiona la solución internamente con los departamentos de la Institución a través de la mesa de ayuda como canal comunicativo o con las empresas que prestan servicios dejando registro del evento, dando paso al "Procedimiento de Monitoreo y Análisis de eventos de seguridad"		Deriva al "Procedimiento de Monitoreo y Análisis de Eventos de Seguridad" para solucionar éste.
0.3	Levantar, clasificar y priorizar Antecedentes e Informar	Jefe del Departamento Gestión de Riesgos de Sistemas de Información	Se levantan los antecedentes relacionados e ingresan en el "formulario de incidentes de seguridad" el detalle del incidente, asignando la criticidad y prioridad de éste. Este formulario posteriormente es enviado a la ESI informando lo sucedido.	0.4	Antecedentes levantados en Formulario de Incidentes de Seguridad e informados mediante correo electrónico
0.4	Iniciar proceso de contacto de Autoridades	Encargado de Seguridad de la Información (ESI)	Recepciona y analiza los antecedentes para Iniciar el proceso de contacto con autoridades.		Proceso de Contacto con Autoridades iniciado
0.5	Establecer causa del incidente	Jefe del Departamento Gestión de Riesgos de Sistemas de Información	En conjunto con Áreas Operativas, investiga y define la causa del incidente, según la criticidad. Completa el formulario de Incidente de Seguridad con estrategia de solución definida.	0.6	Causa del incidente identificado en el Formulario de Incidente de Seguridad

0.5a	Hacer Análisis Forense	Jefe del Departamento Gestión de Riesgos de Sistemas de Información	Se la investigación previa indica que es necesario realizar un análisis forense, se realiza éste y se evacúa un informe.	0.6	Informe forense
0.6	Desarrollar solución y ejecutar solución	Jefes Departamentos DI (áreas operativas)	Una vez identificado, la causa y la criticidad del incidente, el Jefe Departamento de Seguridad de Información (JDSI) coordina el desarrollo y la ejecución de la solución con las áreas operativas que brindan soporte al negocio. El JDSI debe dejar registro de la actividad realizada o implementada en el formulario de Incidente de Seguridad, así como también las evidencias recopiladas. Si la solución definida entrega los resultados esperados, se debe continuar con la actividad 0.7. Si la solución de finida NO entrega los resultados esperados, se debe continuar con la actividad 0.5.	0.7 0.5	Solución registrada o NO solución registrada, en el Formulario de Incidente de Seguridad
	Se soluciona el Incidente	Jefe del Departamento Gestión de Riesgos de Sistemas de Información	De ser solucionado el incidente se actualiza el formulario en base a los nuevos datos recopilados durante la investigación y la implementación de la solución.	0.7	Incidente solucionado en el Formulario de Incidente de Seguridad
	No se soluciona el Incidente	Jefe del Departamento Gestión de Riesgos de Sistemas de Información	- Si el incidente no se ha podido resolver el Jefe del Departamento de Seguridad de información en coordinación con el Jefe de la División, citará a una reunión con los Jefes de Departamentos de la División de Informática y otras áreas que entregan soporte al negocio. Quienes desarrollaran en conjunto la solución del incidente como prioridad máxima dentro de sus funciones. La Minuta Incidentes Graves quedará inserta en el Formulario de Incidente de Seguridad,	0.5	Formulario de Incidente de Seguridad.
0.7	Actualizar antecedentes formularios e informar ESI	Jefe del Departamento Gestión de Riesgos de Sistemas de Información	Debe completar los campos asociados al cierre del incidente del formulario de Incidente de Seguridad y enviarlo al ESI	0.8	Formulario de Incidente de Seguridad actualizado e informada el ESI mediante correo
0.8	Reportar solución	Encargado de Seguridad de la Información (ESI)	Recepciona los antecedentes finales del incidente para su revisión y reporta lo sucedido a lo establecido en el "Procedimiento de Contacto con Autoridades".	Fin del Ciclo	Solución reportada

INSTITUTO DE PREVISION SOCIAL

7. INDICADORES DE GESTIÓN

Responsable de mantener información del indicador: Jefe Departamento Gestión de Riesgos de Sistemas de Información

Nombre 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	Planilla Incidentes

8. CONTROL DE REGISTROS DE OPERACIÓN

La información recopilada en los correos electrónicos y el ticket, descritos en el procedimiento, serán detallados en el "Formulario de Incidente de Seguridad".

Nombre del Registro	Tipo	Responsable	Ubicación	Soporte	Medio de Almacenamiento (Recuperación)	Tiempo de Retención	Disposición
Formulario de Incidente de Seguridad	Documento	Jefe del Departamento Gestión de Riesgos de Sistemas de Información	//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

INSTITUTO DE PREVISIÓN SOCIAL

Evidencias (SÓLO RERERIDOS A INFORMES FORENCE, EN CASO DE EXISTIR)	Documento	Jefe del Departamento Gestión de Riesgos de Sistemas de Información	//DSI/SeguridadIncidentes	Digital	Carpeta digital Incidentes Seguridad	6 años	No aplica

9. ANEXOS

Anexo 1 Formulario de Incidente de Seguridad

El número de registro debe ser paralelo al número de registro de la "Planilla de incidentes".

	FORMULARIO INCIDENTE DE SEGURIDAD			DIVISIÓN DE INFORMÁTICA
	Nivel de Confidencialidad	Uso Interno	Número de Registro	
			Fecha	/ /
			Responsable	Jefe Depto. Gestión de Riesgos de Sistemas de Información

INFORMACION INCIDENTE				
Tipo de Incidente			Criticidad del Incidente	Media
ANTECEDENTES EVENTO				
Ticket Asociado	SI	NO	Correo Asociado	SI NO
VALIDACIÓN				
Identificación de quién reporta				
Que originó el incidente				
Fecha Reporte				
Hora reporte				
Activos / Sistemas afectados				
Descripción				

TRATAMIENTO DEL INCIDENTE			
Responsable de la Acción Inmediata			
Acción Inmediata Realizada			
Fecha Acción Inmediata			
Hora Acción Inmediata			
Descripción:			
TRATAMIENTO DEL INCIDENTE OPCIONAL: (Repetir hasta mitigar el incidente)			
Responsable de la Acción Inmediata			
Acción Inmediata Realizada			
Fecha Acción Inmediata			
Hora Acción Inmediata			
Descripción			
Si el incidente no se ha podido resolver el Jefe del Departamento de Gestión de Riesgos de Sistemas de Información en coordinación con el Jefe de la División, citará a una reunión con los Jefes de las Áreas Operativas de la División de Informática.			
Fecha Reunión	/ /	Numero Minuta Reunión Incidente	

INSTITUTO DE PREVISION SOCIAL V°B° DPTO. CONTROL JURIDICO

Cierre:	
Análisis de Causas	
Costos Asociados	
Acción Correctiva/Preventiva	
Fecha Cierre	
Descripción:	

Parámetro	Descripción	Variables
Criticidad	Importancia del incidente dependiendo de los procesos afectados y usuarios.	Alto: Interrumpe seriamente los procesos de la Institución, afecta a más de cinco funcionarios. Medio: Interrumpe momentáneamente los procesos de la Institución y afecta a más de un funcionario, pero menos de cinco. Bajo: No interrumpe los procesos generales de la Institución y afecta solo un usuario.

	FIRMA JEFE DEPARTAMENTO DE GESTIÓN DE RIESGOS DE SISTEMAS DE INFORMACIÓN			

INSTITUTO DE PREVISIÓN SOCIAL
V°B° DPTO. CONTROL JURÍDICO

Anexo 2 Planilla Incidentes

El número de registro debe ser paralelo al número de registro del "Formulario de Incidente de Seguridad".

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

INFORME INCIDENTE DE SEGURIDAD NUMERO __ __ *RESPONSABLE: Jefe Departamento de Gestión de Riesgos de Sistemas de 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

* N / C = Sin cambio

FIRMA JEFE DEPTO. DE GESTIÓN DE RIESGOS DE SISTEMAS DE INFORMACIÓN

INSTITUTO DE PREVISION SOCIAL V°B° DEPTO. CONTROL JURIDICO

Anexo 3 Guía de evaluación de la criticidad

SEVERIDAD	DESCRIPCIÓN	CRITICIDAD
Alta	a) Afecta gran parte de la Institución b) Impacta activos críticos de la Institución c) Impacta a un gran número de sistemas o personas d) Afecta información confidencial de las personas e) Robo o alteración de los activos de información f) Destrucción de propiedad del IPS g) Aprovechamiento de brechas de seguridad detectadas y no informadas.	INCIDENTE
Media	a) Impacta un número moderado de sistemas o personas b) Impacta activos importantes, pero no críticos c) Puede propagarse a otros activos d) Acceso lógico o físico a sitios no autorizados. e) No informar acerca de brechas en la seguridad detectadas.	EVENTO
Baja	a) Impacta un número pequeño de sistemas o personas b) Afecta un segmento de red c) Baja probabilidad de propagación d) Instalación y/o descarga de software no autorizado. e) Visitas a páginas de Internet no autorizadas.	EVENTO

INSTITUTO DE PREVISIÓN SOCIAL V°B° DPTO. CONTROL JURÍDICO