SE APRUEBA PARA EL INSTITUTO DE PREVISIÓN SOCIAL, EL INSTRUCTIVO INSTITUCIONAL DENOMINADO "PROCEDIMIENTO DE MONITOREO Y ANALISIS DE EVENTOS DE SEGURIDAD"

RESOLUCIÓN EXENTA Nº 289

SANTIAGO, 21 JUN 2016

V I S T O S:

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.

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

1.- Que, resulta necesario establecer el procedimiento de monitoreo con la finalidad de recolectar, analizar, controlar y supervisar los eventos de seguridad de la información y guiar las decisiones para su gestión efectiva y eficiente, minimizando los impactos adversos y asegurando los niveles de servicio y disponibilidad de soluciones oportunas.

2.- Que, para la aplicación general y obligatoria del citado procedimiento, el Subdepartamento de Seguridad de la Información dependiente de la División Informática del Instituto de Previsión Social, ha elaborado el Instructivo Institucional denominado "Procedimiento de Monitoreo y Análisis de Eventos de Seguridad", que incluye la metodología a seguir para implementar la gestión de incidentes de seguridad de la información del Instituto de Previsión Social.

3.- Que, por Oficio Ordinario Nº 45340/2731-16, de 07 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 el correspondiente acto administrativo aprobatorio por el Departamento de Transparencia y Documentación.

R E S U E L V O:

1.- **Apruébase** para el Instituto de Previsión Social, el Instructivo denominado "Procedimiento de Monitoreo y Análisis de Eventos de Seguridad", que consta de dieciséis (16) páginas, que se adjunta como parte integrante de la presente Resolución Exenta, con aprobación legal de fecha 07 de junio de 2016, cuyo objetivo es describir el procedimiento de monitoreo para asegurar la gestión efectiva y eficiente de los eventos de seguridad de la información.

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
DIRECTOR NACIONAL

PATRICIO CORONADO ROJO
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

MTES/YGF/ACA/MVEW/NCR/MEGA/MRC/RRY/rpy
Instructivo "Procedimiento de Monitoreo y Análisis de Eventos de Seguridad"
VI- 15 (Folio DTD 5575-99)

PROCEDIMIENTO DE MONITOREO Y ANALISIS DE EVENTOS DE SEGURIDAD

Elaborador por:	Revisado por:	Aprobado por:
Departamento de Seguridad de la Información	Jefe División Informática - Jefe División Planificación y Desarrollo	División Jurídica Dirección Nacional

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

CONTROL DE CAMBIOS

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

La presente versión substituye completamente a todas las precedentes, de manera que este sea el único documento válido de entre todos los de la serie.

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 (IPS) 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).

VºBº DEPTO CONTROL JURIDICO I.P.S.

INDICE

DEPTO CONTROL JURIDICO I.P.S.

	PROCEDIMIENTO DE MONITOREO Y ANALISIS DE EVENTOS DE SEGURIDAD			DIVISION DE INFORMATICA
	Nivel de Confidencialidad	Uso Interno	Versión	01
			Fecha de Aprobación Legal	07 JUN. 2016
			Página	4 de 16

1. OBJETIVO

Asegurar la gestión efectiva y eficiente a través del monitoreo de los eventos de seguridad; minimizando los impactos adversos y asegurando los niveles de servicio y disponibilidad de la mejor forma posible, definiendo un conjunto de buenas prácticas y desarrollar la metodología a seguir para implementar la gestión de incidentes de seguridad de la información del Instituto de Previsión Social.

2. ALCANCES

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 como punto de partida en el reconocimiento y categorización de los incidentes de seguridad 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: acceso no autorizado a la información.
- Integridad: modificación no autorizada, destrucción o perdida de información.
- Disponibilidad: inaccesibilidad a la información.

3. DOCUMENTOS DE REFERENCIA

- 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 ° 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° 657, del 3 de diciembre de 2015, Política General de Seguridad de la Información del IPS.
- Norma Nch- ISO 27000:2013.
- Norma NCh-ISO 27001:2013:
  - 12.4.1 Registro de evento
  - 16.1.2 Informe de eventos en la seguridad de la información

- Resolución Exenta N°56, 15/02/2016, Política Organizacional de la Seguridad de la Información del IPS.

4.- DEFINICIONES

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

b) **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.

c) **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.

d) **Comité de Seguridad de la Información (CSI):** Grupo integrado por las Jefaturas de 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.

e) **Evento de seguridad de la información:** Corresponde a una ocurrencia identificada que puede ser relevante, el servicio o red, estas instancias indican 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.

f) **Escalar**: Acción que se da cuando el **Departamento de Seguridad de Información** 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 se escapan a su responsabilidad

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.

5.- RESPONSABILIDADES

5.1 Responsabilidades en el Procedimiento

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 Seguridad de Información (DSI):** Son 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 División las correcciones y mejoras necesarias, en el marco del mejoramiento permanente de la gestión.

d) **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 mejora que correspondan y coordinar su implementación.

e) **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.

f) **Encargado de Seguridad de la Información (EDSI):** Es responsable por preservar la confidencialidad, integridad y disponibilidad de la información en IPS. Responsable de velar por el cumplimiento de las políticas de seguridad de la información, sus normas, procedimientos y velar por su correcta aplicación. Establece puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.

Asesora al jefe de servicio en las materias relativas a la seguridad de documentos electrónicos y dirige el Comité de Seguridad de la Información.

g) **Jefe de Seguridad de Información (JDSI):** Es 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.

h) **Mesa de ayuda (MAFIPS):** Recibe reporte, investiga, clasifica, contiene e informa del incidente a las jefaturas y a la Encargada de Seguridad de la Información.

i) **Mesa de Ayuda Departamento Tecnologías, División Informática**: Recibe reporte, investiga, clasifica, contiene e informa del incidente a jefaturas y a la Encargada de Seguridad de la Información.

j) **Centro de Operaciones de Seguridad (SOC):** Es un centro de Operaciones destinado a dar un servicio de seguridad 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.

k) **Superior Jerárquico:** Persona encargada de una División, Departamento o Unidad, quien debe ser informado de los incidentes que ocurren en su División, Departamento o Unidad.

5.2. Responsabilidades de gestión del documento

Departamento de Seguridad de la Información (DSI):

a) Es Propietario o Responsable de la gestión del presente documento, quién tiene la responsabilidad de la administración, actualización, protección y control del ciclo de vida del documento.

6. DESCRIPCIÓN DEL PROCEDIMIENTO

6.1 Descripción de Actividades

Todo el personal del IPS, en coordinación con su jefatura, es responsable de notificar cualquier tipo de evento que pueda afectar el funcionamiento normal del Sistema de Seguridad de la Información la Institución. Esta notificación se hará mediante correo electrónico, con los antecedentes del evento a la Mesa de Ayuda del Departamento de Tecnologías, quien registrará el evento y derivará al Jefe Departamento de Seguridad de la Información.

Según el impacto del evento de Seguridad de Información, el Jefe Departamento de Seguridad de la Información debe contactar a la persona que reporta y Jefatura del área relevante en un plazo no mayor a las 48 horas, para recolectar toda la información necesaria para el análisis del evento, registrando todos los antecedentes en el **Formulario de Registro Evento Seguridad de la Información** (Anexo 1).

Hecha la recolección de información sobre el evento, el Jefe Departamento de Seguridad de la Información debe analizar los antecedentes. El resultado de dicho análisis puede tener las siguientes opciones:

i. El evento no corresponde a una amenaza: se cierra el registro de eventos, informando a la persona que reportó,

ii. El evento corresponde a una incidencia: se gestionan las actividades de mitigación (con los dueños de los activos comprometidos, el área o unidad de competencia y/o Comité Seguridad Información), dejando registro en la Plantilla de tratamientos de eventos.

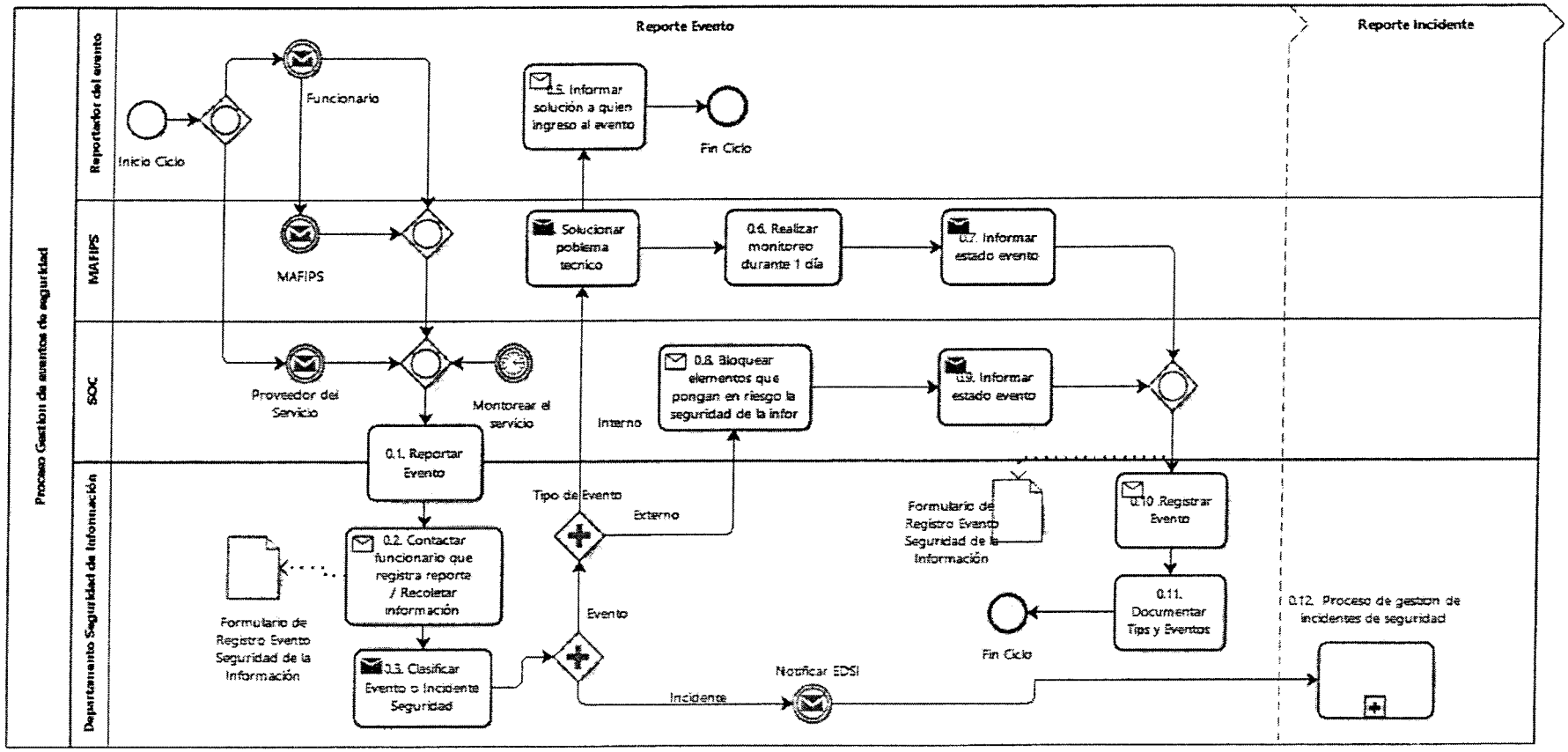
iii. El evento ocurrió y debe ser gestionado como incidente: se activa el proceso de Gestión de Incidentes de Seguridad.

Algunos ejemplos comunes de eventos de seguridad son:

- **Intentos de acceso no autorizado**: acceso físico o lógico por personal no autorizado a recursos de redes, sistemas, aplicaciones o datos de la organización.
- **Intentos de ataques de denegación de servicio (DoS)**: ataque que impide el uso autorizado de las redes, sistemas o aplicaciones mediante el consumo de recursos inapropiado y malicioso
- **Código malicioso**: virus, gusano caballo de Troya o cualquier otro código malicioso que infecta un sistema con consecuencias negativas para la organización
- **Intento de uso inapropiado de recursos**: violación de las normas o políticas establecidas para el uso de los sistemas de información de la organización.
- **Fallas de sistemas:** Sistema deja de operar, se detiene en forma imprevista, envía mensajes programados u otros.

En eventos de gran magnitud que puedan implicar impactos considerados como críticos para el negocio de la organización, deben seguirse las directrices de gestión de incidentes que apliquen y las establecidas por el Plan de Contingencias de la organización que tomarán precedencia sobre las habituales de gestión de incidentes.

6.2 Diagrama de Flujo



6.3 Matriz de Proceso

El proceso se gatilla con el reporte de un evento, que realiza un funcionario a través de las mesas de ayuda o por un evento detectado por el proveedor del servicio, en primera instancia estos eventos son asociados al departamento de seguridad de la información vía correo electrónico y tickets

N°	ACTIVIDAD (Que)	RESPONSABLE (Quién)	DESCRIPCIÓN (Cómo)	Ir	SALIDA
0.1.	Reportar Evento	MESA DE AYUDA (MAFIPS)	El proceso se gatilla con el reporte de un evento, que realiza un funcionario a través de las mesas de ayuda o por un evento detectado por el proveedor del servicio, en primera instancias estos eventos son asociados al departamento de seguridad de la información vía correo electrónico y tickets	0.2.	Correo Electrónico
0.2.	Contactar funcionario que registra reporte	Departamento Seguridad de Información	Se contacta con el funcionario o el proveedor de servicio que reporta evento, se ingresan los antecedentes al formulario de recogida de datos para llevar un control de los eventos	0.3.	Formulario Recogida de datos
0.3.	Clasificar el evento o el Incidente	Departamento Seguridad de Información	Se clasifican los reportes según criticidad e impacto en los sistemas de información y son canalizados según las entidades correspondientes dependiendo, además si es un evento interno o externo se reclasifica en segunda instancia para regularizar con los servicios asociados según corresponda.	0.4. 0.8. 0.12.	Correo Electrónico
0.4.	Solucionar problema técnico	MESA DE AYUDA (MAFIPS)	Realiza solución de evento de soporte en primera instancia	0.5.	Correo Electrónico /Ticket
0.6.	Informa solución a quien ingreso el evento	Funcionario IPS o empresa externa que reporta el evento	Se reporta vía correo o telefónicamente al funcionario la solución de su reporte	0.7.	Correo Electrónico

N°	ACTIVIDAD (Que)	RESPONSABLE (Quién)	DESCRIPCIÓN (Cómo)	Jr.	SALIDA
0.6.	Realizar monitoreo durante 1 día	MESA DE AYUDA (MAFIPS)	Se realiza seguimiento al funcionario y al evento generado	0.7.	
0.7.	Informar estado evento	MESA DE AYUDA (MAFIPS)	Se envía estado del evento y solución realizada al Departamento de Seguridad de Información.	0.8.	Correo Electrónico
0.8.	Bloquear elementos que pongan en riesgo la DSI	SOC	Bloquea u elimina elementos que afecten la continuidad operacional a través de sus plataformas de seguridad	0.9	Correo Electrónico
0.9	Informar estado evento	SOC	Se envía estado del evento y solución realizada al Departamento de Seguridad de Información.	0.10.	Correo Electrónico / Formulario Recogida de datos
0.10.	Registrar Evento	Departamento Seguridad de Información	Evento es registrado en una planilla de control de eventos mensual si es catalogado como un evento crítico.	0.11	Planilla de registros mensual de eventos
0.11	Documentar tips y eventos	Departamento Seguridad de Información	Se crea / actualiza documento que registra eventos más repetitivos, tips y las soluciones realizadas (base de conocimientos)	0.12	Documento
0.12	Proceso de gestión de incidentes de seguridad	Departamento Seguridad de Información	Al ser clasificado como incidente, es notificado vía correo por el Departamento de Seguridad de Información a la Encargada de Seguridad de la Información para iniciar el proceso de gestión de incidentes de seguridad de la información		Correo Electrónico

7. INDICADOR DE GESTIÓN

Nombre Indicador	Fórmula	[illegible]			[illegible]	[illegible]	Registro (medio de verificación)
		Muy satisfactorio	Satisfactorio	Insatisfactorio			
Porcentaje de eventos de seguridad reportados y resueltos en el año.	N° de eventos de seguridad resueltos en el año t / N° Total de eventos de seguridad reportados en el año t) * 100	> 70% y ≤ 100%	> 50% y ≤ 70%	≤ 50%	Mensual	Diciembre	Planilla de registros mensual de eventos

8. CONTROL DE REGISTRO

Nombre del Registro	Tipo	Responsable	Ubicación	Soporte	Medio de Almacenamiento (Recuperación)	Tiempo de Retención	Disposición
Formulario de Registro Evento Seguridad de la Información	Documento	Departamento Seguridad de Información (DSI)	//DSI/MonitoreoEventos	Digital	Carpeta digital Eventos Seguridad	6 años	No aplica
Planilla de registros mensual de eventos	Documento	Encargada Seguridad de la Información (EDSI)	//DSI/MonitoreoEventos	Digital	Carpeta digital Eventos Seguridad	6 años	No aplica
Correo Electrónico Eventos	Correo Electrónico	Departamento Seguridad de Información (DSI)	Carpeta Digital Eventos Correo electrónico	Digital	Carpeta Digital Eventos Correo electrónico	6 años	No aplica

ANEXO A

Anexo 1: Formulario de Registro Evento Seguridad de la Información

	REGISTRO EVENTO SEGURIDAD DE LA INFORMACIÓN		DIVISION DE INFORMATICA
		Número de Registro	XXXXX0000
Responsable	Departamento Seguridad de Información	Fecha y Hora Incidente	DD.MM.2016 HH:MM
INFORMACIÓN EVENTO			
Nombre Usuario			
Teléfono del Usuario			
Email del Usuario			
INFORMACIÓN DEL EVENTO			
Fecha y Hora de Contacto			
Descripción del problema			
Pagina/máquina donde ha sido detectado el problema			(Opcional)
Software Utilizado por el usuario			(Opcional)
Descripción mínima del equipo			(Opcional)
Forma de Acceso			(Opcional)
Que ha estado haciendo justo antes			(Opcional)
¿Ha tratado de repetir la operación y ha sucedido lo mismo	SI (X)	NO (X)	
Ha sucedido más de una vez	SI (X)	NO (X)	
EL EVENTO PASO A SER INCIDENTE DE SEGURIDAD	SI (X)	NO (X)	
Causa:			

NOMBRE RECEPTOR

FIRMA RECEPTOR

Anexo 2: Guía para la clasificación de incidentes

Las siguientes categorías podrían utilizarse para la clasificación de incidentes:

NOMBRE	EJEMPLO
Exposición de datos personales	Se han revelado datos personales confidenciales.
Denegación de servicio	Actividad maliciosa tendiente a dificultar el acceso a un servicio.
Actividad de software malicioso	Virus, worms, keylogger, phishing.
Violación de políticas de seguridad	Uso inapropiado de recursos.
Servicios no autorizados	Servicio ftp no autorizado.
Acceso no autorizado	Abuso de privilegios.

2.1 Guía de evaluación de la criticidad de un incidente

SEVERIDAD	DESCRIPCIÓN
Alto	Afecta gran parte de la Institución Impacta activos críticos de la Institución Afecta información confidencial de las personas Amenaza la vida de las personas Robo o alteración de información crítica. Destrucción de propiedad del IPS Aprovechamiento de brechas de seguridad detectadas y no informadas.
Medio	Impacta un número moderado de sistemas o personas Impacta activos importantes pero no críticos Puede propagarse a otros activos Acceso lógico o físico a sitios no autorizados. No informar acerca de brechas en la seguridad detectadas.
Bajo	Impacta un número pequeño de sistemas o personas Afecta un segmento de red Baja probabilidad de propagación Instalación y/o descarga de software no autorizado. Visitas a páginas de Internet no autorizadas.