OFICINA DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN.

Manual de Incidentes de Seguridad de la Información

Diciembre 2020

1. OBJETIVO

Este documento proporciona una guía para la gestión de los diferentes tipos de incidentes de Seguridad de la Información que puedan llegar a presentarse en el Ministerio de Educación Nacional. El manual involucra la forma de preparar, detectar, contener, erradicar, recuperar y hacer seguimiento de los incidentes de seguridad de la información que lleguen afectar a la Entidad, además de cumplir las especificaciones y prácticas del Sistema de Gestión de Seguridad de la Información.

2. ALCANCE

La atención y gestión de los incidentes de seguridad de la información aplica para todos los Activos de Información del Ministerio, sin importar que se encuentren clasificados o no.

Aplica para todos los servidores de planta y provisionales, contratistas y terceros que tengan acceso a los activos de información.

El presente documento contiene los componentes generales de la gestión de incidentes, sus principales acciones las cuales son aplicables indistintamente de la plataforma operacional, tipo o activos de información sobre el cual se presente y/o exista un indicio de incidente de seguridad.

Inicia con la preparación antes de la presencia de un incidente de seguridad de la información y finaliza con las lecciones aprendidas y seguimiento.

3. GENERALIDADES

3.1 POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

El Ministerio de Educación Nacional, reconoce la importancia de gestionar los incidentes de seguridad de la información, como un mecanismo para asegurar la protección de la información por lo tanto esta política declara:

- Se deben adoptar medidas y/o mecanismos necesarios y eficientes para proteger los activos de información.
- Se deben analizar los eventos de seguridad de la información a través de los mecanismos necesarios para tratar de determinar la presencia de un incidente de seguridad de la información
- Verificar la ejecución de o los procedimientos que se tengan definidos para contener y mitigar el incidente que se presenta.
- Documentar y clasificar los incidentes de seguridad de la información que se presenten en la entidad.
- Documentar las lecciones aprendidas durante el incidente.
- Aprender de los incidentes de seguridad de la información con el objetivo de prevenir nuevas ocurrencias.

- Reportar a la Oficina de Tecnología y Sistemas de Información a través del mecanismo definido la presencia de incidentes de seguridad de la información.
- Validar con las áreas involucradas que las consecuencias de los incidentes presentados hayan sido reparadas.
- Emprender acciones post-incidentes con el objetivo de realizar mejoras a los procedimientos operativos de gestión de incidentes de seguridad de la información.

- Emprender acciones cuando se requieran en materia de retención de evidencia digital.

3.2 DEFINICIONES

Dentro de la atención de incidentes de seguridad de la información es importante clarificar algunos conceptos con los cuales se define el procedimiento de gestión de incidentes. Entre ellos se encuentran:

3.2.1 Evento de Seguridad de la Información

Un evento de seguridad de la información es la ocurrencia identificada de un estado del sistema, servicio o red que indica una posible violación a la política de seguridad de la información, una falla de los controles, o una situación desconocida que puede ser relevante para la seguridad de la información.

3.2.2 Incidente de Seguridad de la Información - ISI

Se entiende por incidente de seguridad de la información, todo evento o grupo de eventos adversos o no esperados en materia de seguridad de la información que tiene una probabilidad importante de comprometer las operaciones del negocio y amenazar los pilares de la seguridad de la información, integridad, confidencialidad y disponibilidad.

Para el Ministerio y dentro del espectro tan amplio que involucra la definición, los incidentes se contemplan dentro de los siguientes tipos:

- ✓ ***Acceso No Autorizado:*** El acceso no autorizado a la información o los recursos tecnológicos involucra todas aquellas actividades en las que sin autorización específica o que no se encuentre dentro de las funciones del usuario, se pueda utilizar la información o cualquier activo de información, bien sea de manera intencional o no, o en su defecto se explote una debilidad sobre la información y/o activo de información, con la cual se realicen operaciones no autorizadas, inesperadas o indebidas. Hacen parte de esta categoría:

  - Accesos no autorizados exitosos, sin o con perjuicios visibles a los componentes tecnológicos.
  - Robo de información.
  - Borrado de información.
  - Alteración de la información.
  - Intentos recurrentes y no recurrentes de acceso no autorizado.
  - Abuso y/o mal uso de los servicios informáticos internos o externos que requieren autenticación.

- ✓ ***Código Malicioso:*** Se entiende por código malicioso todos aquellos programas como virus, troyanos, gusanos, y algún otro tipo de programa o scripts que tiene como propósito afectar un sistema informático o en si misma a la información, de tal forma que pueda corromper, alterar, modificar y/o destruir la información. Hacen parte:

  - Virus informáticos.
  - Troyanos.
  - Gusanos informáticos.
  - Keyloggers, Screenloggers, Mouseloggers.
  - Spyware, Rootkits.

- ✓ ***Denegación de Servicio:*** Esta categoría incluye los eventos que ocasionan pérdida de un servicio, en nuestro caso, se considera esta clasificación cuando los usuarios autorizados a la información, o activos de información de la organización no pueden hacer uso de dichos recursos y la falla no es atribuible a problemas de operación normal. Dentro de este marco se contemplan las denegaciones de servicios a:

  - Servicio de correo electrónico.
  - Interrupción de la red de transmisión de datos.
  - Interrupción de Servicios WEB y/o Portales WEB.
  - Interrupción de los Sistemas de Información.

- ✓ ***Mal Uso o abuso de los Recursos Tecnológicos:*** Esta categoría agrupa los eventos que atentan contra los recursos tecnológicos por el mal uso. Comprende:

  - Utilización del recurso correo electrónico para temas como: Spam, Phishing, Hoax, cadenas de correo.
  - Utilización del recurso como el correo electrónico, e Internet para temas como: Contenido pornográfico, divulgación de información reservada o propia del Ministerio sin debida autorización.
  - Utilización de la red para temas como: Realización de pruebas de intrusión, Scan, o vulnerabilidades, sin autorización.
  - Robo, fuga, espionaje o perdida de información para temas como: Medios externos de almacenamiento, transporte de material impreso.
  - Violación de las políticas, normas y procedimientos de seguridad de la información.
  - Uso inadecuado de las Redes Sociales.

- ✓ ***Análisis de Vulnerabilidades:*** Esta categoría agrupa todas las posibles fallas que puedan afectar a los sistemas y dentro de las cuales las causas de dichas vulnerabilidades se deben a fallas de los productos, de las configuraciones de los servicios o de diseño de la infraestructura tecnológica, para ello la Oficina de Tecnología y Sistemas de la Información realiza pruebas de vulnerabilidad periódicamente sobre la infraestructura tecnológica de la organización, identificando este tipo de vulnerabilidades.

3.2.3 Gestión de Incidentes de Seguridad de la Información (GISI)

Para el Ministerio la gestión de incidentes de seguridad de la información consiste en mantener un programa de atención oportuno, eficaz y eficiente de incidentes de seguridad sobre la información; de manera que se obtenga suficiente y objetiva evidencia del hecho, con el propósito de prevenir, detectar, y arreglar las fallas en la seguridad de la información.

La gestión de incidentes involucra el siguiente conjunto de actividades frente a un incidente:

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

Cabe aclarar que la gestión de incidentes de seguridad de la información no es una labor de ejecución unitaria de la Oficina de Tecnología y Sistemas de Información, sino un trabajo en donde deben involucrarse otras áreas como la Subdirección de Desarrollo Organizacional, , la Oficina de Control Interno, Unidad de Atención al Ciudadano (Grupo de Gestión Documental), la alta dirección y los dueños y custodios de la información o activos de información, pues deben ser ellos quien en algún momento realicen las operaciones de configuraciones, cambios y suministro de información al momento de tratar un incidente de seguridad de la información.

4. ROLES PERFILES Y RESPONSABILIDADES

A continuación, se describen los perfiles y responsabilidades de quienes pueden intervenir ante un incidente de seguridad de la información dentro de la organización mediante una matriz RACI:

Actividades	**Mesa Técnica SGSI**	**Oficina de Tecnología y Sistemas de Información**	**Unidad de Atención al Ciudadano (G. Documental)**	**Control Interno**	**Subdirección de Desarrollo Organzaicional**	**Servidores y Contratistas**	**Oficina Asesora Jurídica y SG(Disciplinarios)**
Definir y difundir la Política y el procedimiento de Gestión de Incidentes de Seguridad de la Información.	**I**	**A,R**	**IC**	**I**	**C,I**	**I**	
Atender Incidentes de Seguridad de la Información.		**A,R**	**AR**	**I**	**I**		
Reportar Incidentes de Seguridad de la Información.	**I**	**A,R**	**AR**	**I**	**I**	**R**	

Actividades	**Mesa Técnica SGSI**	**Oficina de Tecnología y Sistemas de Información**	**Unidad de Atención al Ciudadano (G. Documental)**	**Control Interno**	**Subdirección de Desarrollo Organzaicional**	**Servidores y Contratistas**	**Oficina Asesora Jurídica y SG(Disciplinarios)**
Gestionar y asignar recursos para una adecuada Gestión de la Seguridad de la Información.	**I**	**A,R I**	**AR**	**I**	**I**	**I**	
Realizar informes de la Gestión de Incidentes de Seguridad de la Información presentados.	**I**	**A,R**	**I**	**I**	**C**		
Informar las instancias internas correspondientes, los indicentes que puedan requerir alguna medida disciplinaria o penal.		**A,R**		**I**	**I**		**C**
Realizar la gestión correspondiente a las medidas disciplinarias o penales y el respectivo seguimiento.		**I**		**RA**			**RA**

Matriz 1. RACI: Roles y Responsabilidades en la Gestión de Incidentes de Seguridad de la Información.

Una Matriz RACI identifica:

- Responsable (R)
-
- Debe rendir cuentas (A)
- Debe ser consultado (C)
- Informado (I).

5. METODOLOGIA

El Ministerio cuenta con un proceso de cinco (5) fases para la Gestión de Incidentes de Seguridad de la Información, los cuales permiten gestionar un incidente desde el momento antes de la ocurrencia del incidente hasta la forma en cómo se debe aprender y obtener la experiencia y bases de conocimiento para eventos futuros:

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

5.1 Fase 1: Preparación

La fase de preparación, comprende las medidas que se encuentran implementadas y dispuestas para anticiparse a la ocurrencia de los incidentes de seguridad de la información, con las cuales se repelen que pueden llegar a presentarse, adicional a ello se han aplicado las mejores prácticas para el manejo de los recursos tecnológicos y de la información.

A continuación, se relacionan los diferentes tipos de incidentes que se presentan en la plataforma tecnológica y las herramientas con las que cuenta la entidad para que estos puedan ser detectados:

Proxys se debe eliminar de la tabla y complementar con herramientas de gestión documental.

TIPOS DE INCIDENTES DE PLATAFORMA TECNOLÓGICA	HERRAMIENTAS							
	FIREWALL PERIMETRAL				PROXY	ANTIVIRUS/ ANTI-MALWARE	CONTROL DE ACCESO	NESSUS
	IDS/IPS	ANTIVIRUS	ANTIMALWARE	FIREWALL				
Acceso No Autorizado	X			X	X			
Código Malicioso		X	X		X	X		
Denegación de Servicios	X			X				
Mal Uso o Abuso de los Recursos Tecnológicos					X		X	
Análisis de Vulnerabilidades								X

Matriz 2. Incidentes de Seguridad de la Información Vs. Herramientas de Detección.

En esta fase se definen los lineamientos básicos con los cuales se afrontan los incidentes de seguridad de la información que se presentan dentro de la plataforma tecnológica del Ministerio. De la misma manera, se ha establecido como línea base de defensa la formulación de la atención de dichos incidentes a través de esta metodologia la cual se concentra en las herramientas con las que se cuenta para identificar dichos incidentes de seguridad de la información.

5.1.1 Firewall Perimetral

La Entidad cuenta con un Firewall Perimetral que ofrece una combinación ideal de tecnologías de seguridad, implementación y administración. Este appliance ofrece un conjunto completo de características de seguridad perimetral incluyendo firewall, prevención de intrusiones, antivirus, Anti-Spam y filtrado Web, así como VPN's seguras de sitio a sitio y conectividad de acceso remoto.

5.1.2 Antivirus / Antimalware

El Antivirus/Anti-Malware gestiona los incidentes de seguridad basado en una infraestructura centralizada, la cual proporciona protección en estaciones de trabajo y los servidores.

Esta infraestructura integra:

- ***Antivirus.*** Además de la detección basada en firmas, proporciona la detección heurística que emula una máquina virtual dentro del equipo, comprobando todos los archivos y códigos en busca de comportamiento malicioso. Esta técnica produce menos falsos positivos y tasas de detección significativamente más altas para amenazas desconocidas y de "día cero".

- ***Antispyware.*** La herramienta detecta y previene el spyware y adware conocidos a través de diversos métodos de filtrado diferentes para prevenir las infecciones por spyware que puedan causar fuga de información.

- ***Troyanos y rootkits.*** Pueden ser detectados por el motor de análisis de la Herramienta de Antivirus/Anti-Malware.

5.1.3 *Control de Acceso*

El control de acceso a la infraestructura tecnológica por parte de todos los servidores funcionarios de planta y contratistas del Ministerio es realizado por la Oficina de Tecnología y Sistemas de Información de acuerdo con las necesidades de los usuarios.

5.1.4 Herramienta de Identificación de Vulnerabilidades

Las herramientas utilizadas para el análisis de vulnerabilidades se ejecutan periódicamente y sus resultados se presentan en reunión de seguimiento de pares de seguridad informática con una periodicidad de cada tres meses. Esta actividad ayuda a la identificación de los componentes críticos, débiles o susceptibles a daños y/o interrupciones; así como a la generación de medidas de emergencia y/o mitigación para que éstas sean implementarse ante las amenazas previamente identificadas.

5.2 Fase 2: Detección

La fase de detección involucra la identificación del incidente de seguridad de la información y donde se lleva a cabo las actividades de:

- Validar si de acuerdo con los lineamientos definidos anteriormente el incidente se considera de seguridad de la información.
- Clasificar el incidente.
- Reportar el incidente ante las personas, áreas y/o autoridades que correspondan.

Esta fase involucra la atención del incidente, se encuentra definida en una escala de tiempo (Horas y días), encontrándose estrechamente relacionada de acuerdo con su clasificación, dicha escala se encuentra definida como el tiempo máximo que puede tardarse en atender o poner en marcha la gestión de atención de incidentes de seguridad de la información, pero no necesariamente en dar su respuesta:

5.2.1 *Tiempo de Atención de un ISI*

*Tipo	Calificción del Incidente	Acuerdo de Servicio (OLA)	
		Tiempo de Atención	Tiempo de Solución
1	Muy Grave (9-10)	4 horas	1 día
2	Grave (7 – 8)	5 horas	2 días
3	Normal (5- 6)	8 horas	3 días
4	Poco Importante (3 – 4)	1 día	5 días
	No importante (1 - 2)	2 días	7 días

Matriz 3. Clasificación y niveles de atención de incidentes

Las categorías numéricas y cualitativas del incidente son parámetros definidos por el Ministerio para tener una facilidad en su manejo.

* El tipo corresponde a la categoría asignada en la herramienta establecida por el Ministerio.

5.2.2 Herramienta de Identificación de Vulnerabilidades

La categoría del incidente es dada por la herramienta de análisis de vulnerabilidades y validada con las categorías señaladas en el numeral anterior.

Calificación del Incidente	Equivalencia Herramienta de Vulnerabilidad	Escala de Tiempo para Presentación del Plan
Muy Grave (9-10)	Crítico con Exploit	7 días
Grave (7 – 8)	Crítico sin Exploit Severo con Exploit	7 días
Normal (5- 6)	Severo sin Exploit	7 días
Poco Importante (3 – 4)	Moderado Con Exploit	7 días
No importante (1 - 2)	Moderado Sin Exploit	7 días

Matriz 4. Clasificación y niveles de atención de incidentes Herramienta de Análisis de Vulnerabilidades.

Para la actividad de identificación y reporte de los incidentes a los niveles adecuados se debe tener en cuenta la siguiente información, a continuación, se realiza una breve explicación de la tabla:

Escenario: Hace referencia a los diferentes tipos de incidentes de seguridad de la información definidos por la organización.

Criticidad: Hace referencia a la calificación del incidente.

Fuentes de Datos: Hace referencia a los diferentes dispositivos que soportan la infraestructura de seguridad de la organización.

Origen: Hace referencia al punto donde se origina el incidente de seguridad de la información, este puede ser una estación de trabajo y/o un servidor.

Roles Notificados: Hace referencia a los roles involucrados en esta fase de la gestión de incidentes de seguridad de la información; se realiza una pequeña matriz RACI donde se especifica quien es el **R**esponsable (**R**), quien debe rendir cuentas(**A**), quien debe ser **C**onsultado(**C**) y/o **I**nformado(**I**) en los diferentes escenarios y orígenes.

Tiempo de Atención: Hace referencia al tiempo subjetivo de servicio definido por la Organización y las Áreas involucradas.

ESCENARIO	CRITICIDAD	FUENTES DE DATOS					ORIGEN		ROLES NOTIFICADOS					Tiempo de Acción
		PROXY	ANTIVIRUS ANTIMALWARE	CONTROL DE ACCESO	ESCANEO VULNERABILIDADES	FIREWALL PERIMETRAL	Estación de Trabajo	Servidor	OTSI	SDO	Soporte Técnico	Usuarios/ Jefes	Control Interno	
Código Malicioso	Poco importante hasta Normal	X	X			X	X				R			<=10 Días
	Grave hasta muy Grave	X	X			X	X			A	R			<=2 Días
	Poco importante hasta Normal	X	X			X		X	R					<=10 Días
	Grave hasta muy Grave	X	X			X		X	R	A				<=2 Días
Acceso No Autorizado	Poco importante hasta Normal	X				X	X				R			<=10 Días
	Grave hasta muy Grave	X				X	X		C	A	R			<=2 Días
	Poco importante hasta Normal	X				X		X	R					<=10 Días
	Grave hasta muy Grave	X				X		X	R	A				<=2 Días
Uso Indebido de la información y recurso tecnológico	Poco importante hasta Normal	X		X			X		C	A		I		<=10 Días
	Grave hasta muy Grave	X		X			X		C	A		I	C	<=2 Días
Denegación de Servicios	Grave hasta muy Grave					X		X	R	A		I	I	<=2 Días
Análisis de Vulnerabilidades	Poco importante hasta Normal				X			X	R	A			I	<=10 Días
	Grave hasta muy Grave				X			X	R	A		C	I	<=2 Días

Matriz 5. Fase 2: Reportes de Incidentes de acuerdo con el tiempo de acción

5.3 Fase 3: Contención

La contención como su nombre lo indica, hace referencia en contener el impacto o efecto que un incidente de seguridad de la información puede llegar a tener dentro de la infraestructura y arquitectura de la organización.

Es de carácter obligatorio que siempre existan notificaciones sobre las acciones emprendidas, que serán registradas a través de la mesa de ayuda de tecnología y de los planes de mitigación de vulnerabilidades, por lo tanto, se hace indispensable esta información.

A continuación, se realiza una breve explicación de la tabla:

Escenario: Hace referencia a los diferentes tipos de incidentes de seguridad de la información definidos por la Organización.

Criticidad: Hace referencia a la calificación del incidente.

Origen: Hace referencia al punto donde se origina el incidente de seguridad de la información, este puede ser una estación de trabajo y/o un servidor.

Roles Notificados: Hace referencia a los roles involucrados en esta fase de la gestión de incidentes de seguridad de la información; se realiza una pequeña matriz RACI donde se especifica quien es el **R**esponsable (**R**), quien debe rendir cuentas(**A**), quien debe ser **C**onsultado(**C**) y/o **I**nformado(**I**) en los diferentes escenarios y orígenes.

Actividades de Contención: Hace referencia a las actividades realizadas en los diferentes escenarios para el desarrollo de esta fase.

ESCENARIO	CRITICIDAD	ORIGEN		ROLES NOTIFICADOS								
		Estación de Trabajo	Servidor	OTSI	SDO	Soporte Técnico	Jefes Necesarios	Control Interno	Recursos Humanos	Seguridad Física	Propietario del Activo	Área Jurídica
Código Malicioso	Poco importante hasta Normal	X			A	R						
	Grave hasta muy Grave	X			A	R					C	
	Poco importante hasta Normal		X	R	A							
	Grave hasta muy Grave		X	R	A						C	
Acceso No Autorizado	Poco importante hasta Normal	X				R						
	Grave hasta muy Grave	X		C	A	R					C	
	Poco importante hasta Normal		X	R								
	Grave hasta muy Grave		X	R	A		I				C	
Uso Indebido de la información y recurso tecnológico	Poco importante hasta Normal	X		C	A		I	C		C		
	Grave hasta muy Grave	X		C	A		C	C	C	C		C
Denegación de Servicios	Grave hasta muy Grave		X	R	A		I	I			I	
Análisis de Vulnerabilidades	Poco importante hasta Normal		X	R	A		C					
	Grave hasta muy Grave		X	R	A		C					

Matriz 6. Fase 3: Personal y Actividades sugeridas para desarrollar en cada escenario de incidentes.

5.4 Fase 4: Erradicación y Recuperación

En esta fase se busca remover las causas del incidente e identificar las actividades de recuperación que se deben llevar a cabo para lograr mejoramiento en los procesos y actividades realizadas para salvaguardar la seguridad de la información.

Es importante para esta fase que se determinen las siguientes acciones de erradicación del incidente de seguridad de la información y se garanticen las operaciones de recuperación.

A continuación, se realiza una breve explicación de la tabla:

Escenario: Hace referencia a los diferentes tipos de incidentes de seguridad de la información definidos por la Organización.

Actividades de Erradicación: Hace referencia a las actividades realizadas en los diferentes escenarios para el desarrollo de esta fase.

Actividades de Recuperación: Hace referencia a las actividades realizadas en los diferentes escenarios para el desarrollo de esta fase.

E: Actividad de Erradicación.

R: Actividad de Recuperación.

ESCENARIOS					**Actividades de Erradicación**
Código Malicioso	Acceso no autorizado	Uso indebido de la Información y los Recursos Tecnológicos	Denegación de Servicios	Análisis de Vulnerabilidades	
E	**E**	**E**	**E**		Identificar las causas del incidente, eliminándolas completamente.
E	**E**		**E**	**E**	Buscar mejoras en los esquemas de protección actuales.
	E		**E**		Realizar pruebas de vulnerabilidad para revisar el estado final una vez que haya sido superado el incidente de seguridad de la información.
					En caso de ser necesario, restaurar el sistema o reinstalarlo por completo.

Matriz 7. Actividades sugeridas para la Erradicación en cada escenario de incidentes.

ESCENARIOS					Actividades de Recuperación
Código Malicioso	Acceso no autorizado	Uso indebido de la Información y los Recursos Tecnológicos	Denegación de Servicios	Análisis de Vulnerabilidades	
R	**R**		**R**		Recuperación de los datos y configuraciones.
R	**R**		**R**		Realizar procesos de actualización.
	R	**R**	**R**	**R**	Mejorar los procesos y procedimientos.
			R		Mejorar los niveles de auditoría.

Matriz 8. Actividades sugeridas para la Recuperación en cada escenario de incidentes.

5.5 Fase 5: Seguimiento

Esta fase involucra comprobar que todo realmente vuelve a la normalidad, y además se mantenga de la misma manera o mejor hasta una nueva eventualidad.

El responsable de realizar el seguimiento de los Incidentes de Seguridad de la Información es la Oficina de Tecnología y Sistemas de Información, quien realizará informes gerenciales al Comité Institucional de Gestión y Desempeño trimestralmente y se medirá la gestión mediante los indicadores definidos.

La documentación de los incidentes se realizará mediante herramienta establecida por el Ministerio, a excepción del análisis de vulnerabilidades que se realiza mediante informes presentados por el operador de servicios TIC.

6. CUMPLIMIENTO

Todos los servidores del Ministerio deben cumplir y acatar la política de gestión de incidentes de seguridad de la información, así como los procedimientos y prácticas derivadas de la misma. Corresponde realizar seguimiento a su estricto cumplimiento a la Oficina de Tecnologia y Sistemas de Información.

El incumplimiento de todos y cada uno de los documentos en esta materia, podrá ser sancionado, conforme lo establece la normativa vigente.

7. SEGUIMIENTO Y MEDICIÓN

El seguimiento se realiza a través de la reunión de pares de seguridad informática y las Mesas Técnicas de Seguridad Digital en donde se abarcan temas relacionados con el Modelo de Gobierno de Seguridad de la Información para el Ministerio, se revisa que la Seguridad de la Información se encuentre alineada con los objetivos de Negocio, se realiza seguimiento a los incidentes de seguridad de la información, entre otros temas, y esto se deja evidenciado en el acta de este comité.

La medición se realiza mediante los indicadores definidos por la Oficina de Tecnología y Sistemas de Información , los cuales nos permiten medir la eficiencia de las herramientas con las que cuenta la Entidad para detectar un incidente y el equipo de personas para tratarlo. A continuación, se definen las metas correspondientes a la medición:

Tipo de Indicador	Objetivo	Requerimiento ISO-IEC 27001 / Objetivo de Control ISO-IEC 27002	Indicador	Tipo			Fórmula	Frecuencia de Medición	Meta		
				Eficacia	Eficiencia	Efectividad			Inaceptable	Tolerable	Aceptable
Táctico	% de Incidentes Graves hasta Muy Graves cerrados.	13.1.1 Reporte sobre los eventos de seguridad de la información. 13.1.2 Reporte sobre las debilidades en la seguridad.	Porcentual (%)		x		***Pki(i)***=[Total de Incidentes Graves hasta Muy Graves Cerrados / Total de Incidentes Identificados] * 100	Mensual	P(i) > 95%	100% >= P(i) <= 95%	P(i) = 100%
	% de Incidentes Poco Importante hasta Normal cerrados.	13.1.1 Reporte sobre los eventos de seguridad de la información. 13.1.2 Reporte sobre las debilidades en la seguridad.	Porcentual (%)		x		***Pki(i)*** = [Total de Incidentes Poco Importantes hasta Normal Cerrados / Total de Incidentes Identificados] * 100	Mensual	P(i) > 85%	90% >= P(i) <= 85%	100% >= P(i) < 90%

8. FORMATOS / EVIDENCIAS

- Registro y reportes de la atención de incidentes de seguridad de la información a través de la herramienta dispuesta por el Ministerio, actas de las reuniones de pares de seguridad informática las cuales se celebrarán mensualmente y actas de las Mesas Técnicas de Seguridad Digital

9. Control de Cambios		
Versión	**Fecha de entrada en vigencia**	**Naturaleza del cambio**
01	El documento entra en vigencia a partir de su publicación en el SIG	De acuerdo con la revisión entre la OTSI y SDO de migración documental del SGSI del Proceso de Gestión de Procesos y Mejora al Proceso de Gestión de Servicios TIC, se actualiza y crea este manual en el proceso de Gestión de Servicios TIC el cual se encontraba en el proceso de Gestión de Procesos y Mejora con el código PM-MA-02

10. Ruta de aprobación					
Elaboró		**Revisó**		**Aprobó**	
Nombre	Luis Carlos Serrano Pinzon	**Nombre**	Lina Durán	**Nombre**	Roger Quirama Garcia
Cargo	Contratista – responsable del Sistema de Gestión de Seguridad de la Información / OTSI	**Cargo**	Profesional Especializado SDO	**Cargo**	Jefe OTSI