1. Objetivo, alcance y convenciones

Objetivo	Gestionar de manera eficaz y oportuna los incidentes de Seguridad de la Información que se presenten en el Ministerio de Educación Nacional con el propósito de conservar la Confidencialidad, Integridad y Disponibilidad de sus Activos de Información.
Alcance	Inicia con la detección y reporte de los incidentes de seguridad de la información y finaliza con el seguimiento y cierre de los mismos.

Convenciones	**Punto de Verificación**	**Nota**	**Evidencias**	**Interacción con otros procesos**	**Tiempos**	
					Mínimo	**Máximo**
						

2. Disposiciones Generales

1. POLITICAS GENERALES

- El horario de atención de la Mesa de Servicios es de lunes a sábado entre las 7:00 a.m. y las 9:00 p.m. en jornada continua.
- Todo Incidente debe reportarse por cualquiera de los canales válidos y disponibles: (Llamada telefónica, correo electrónico, registro web o herramienta de gestión CA Service Desk) y debe generar un registro en la herramienta de gestión CA Service Desk.
- Reportar de forma inmediata de acuerdo con el procedimiento previsto los eventos, incidentes o debilidades en cuanto a la seguridad de la información que identifiquen o se presenten.
- Evaluar cada evento o incidente de seguridad de la información presentado en el MEN, usando la escala de clasificación de incidentes de seguridad de la información con el fin de poder determinar clasificación y priorización de acuerdo con lo definido en el manual ST-MA-04_V1.

2. Disposiciones Generales

- Registrar los resultados de la evaluación y la decisión para referencia y verificaciones futuras (Lecciones aprendidas).
- Responder a los incidentes de seguridad de la información que se presenten en el MEN. La respuesta debe incluir:

  - ✓ Recolectar evidencia lo más pronto posible después de que ocurra el incidente.
  - ✓ Llevar a cabo análisis forense de seguridad de la información, según se requiera.
  - ✓ Llevar el asunto a una instancia superior, según se requiera.
  - ✓ Asegurarse de que todas las actividades de respuesta involucradas se registren adecuadamente para análisis posterior.
  - ✓ Comunicar la existencia del incidente de seguridad de la información o de cualquier detalle pertinente a él, al personal interno o externo y a las organizaciones que necesitan saberlo.
  - ✓ Tratar las debilidades de seguridad de la información que se encontraron, que causaron o contribuyen al incidente.
  - ✓ Una vez que el incidente se haya tratado lo suficiente, cerrarlo formalmente y hacer un registro de esto.
  - ✓ Escalar los incidentes a niveles superiores o control interno en caso de que sea requerido.

- Documentar todos los incidentes de seguridad de la información reportados en el MEN.
- Llevar una bitácora de los incidentes de seguridad de la información reportados y atendidos en el MEN por medio del aplicativo dispuesto para tal fin.
- Tener en cuenta que los procedimientos para evidencia deben contener actividades tales como: identificación, recolección, adquisición, y preservación de evidencia de acuerdo con los diferentes tipos de medios, dispositivos y estado de los dispositivos (encendidos o apagados, por ejemplo). Los procedimientos deben tener en cuenta:

  - ✓ La cadena de custodia.
  - ✓ La seguridad de la evidencia.
  - ✓ La seguridad del personal.
  - ✓ Los roles y responsabilidades del personal involucrado.
  - ✓ La competencia del personal.
  - ✓ La documentación.
  - ✓ Las sesiones informativas.
  - ✓ Para el transporte de elementos se debe llevar la cadena de custodia.

2. Disposiciones Generales

IMPORTANTE: 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.

Así mismo, su atención y tratamiento dependerá de los diferentes frentes y especialistas encargados de administrar todas las herramientas y equipos en donde se almacene la información de la entidad.

2. TÉRMINOS Y DEFINICIONES

- **ACTIVO DE INFORMACIÓN:** Es todo aquello que en el Ministerio de Educación Nacional es considerado importante o de alto valor para la entidad, porque contiene información importante, como son los datos creados o utilizados por procesos de la organización, en medio digital, en papel o en otros medios. Ejemplos: bases de datos con usuarios, contraseñas, números de cuentas, informes etc.

- **CONFIDENCIALIDAD:** Propiedad de la información que pretende garantizar que esta sólo es accedida por personas o sistemas autorizados.

- **DATO:** Es una representación simbólica (numérica, alfabética, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.

- **DISPONIBILIDAD:** Propiedad de la información que pretende garantizar el acceso y uso de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

- **EVENTO DE SEGURIDAD:** Ocurrencia identificada de una condición de un proceso, sistema, servicio, red o del entorno que indica una posible violación de las políticas de seguridad de la información del Ministerio de Educación Nacional, o una falla en los controles o situación previamente desconocida que puede ser relevante para la seguridad de la información.

2. Disposiciones Generales

- **INFORMACIÓN:** Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

- **INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN:** Uno o más eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones de la entidad y amenazan la confidencialidad, integridad y/o disponibilidad de la información del Ministerio de Educación Nacional.

- **INTEGRIDAD:** Propiedad de la información que pretende mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

- **SEGURIDAD DIGITAL:** Es el área de la informática que se enfoca en la protección de la infraestructura computacional, todo lo relacionado con esta y, especialmente, en la información contenida o circulante. Incluye la seguridad de la información (Políticas, Procedimientos y demás controles) y la seguridad informática (Herramientas de seguridad).

- **SGSI:** Sistema de Gestión de Seguridad de la Información.

3. MATRIZ RACI

Actividades	Usuarios Internos / Externos MEN	Analista Mesa de Ayuda	Responsable de SI OTSI - MEN	Grupo Respuesta a ISI - MEN
Reportar Incidente de Seguridad de la Información.	R			
Evaluar Incidente de Seguridad de la Información.		R	R	

2. Disposiciones Generales

Crear, categorizar y priorizar el Incidente de Seguridad de la Información.		R	A	C
Escalar Incidente de Seguridad de la Información		R	R	
Realizar Contención del Incidente de Seguridad de la Información.			A/C	R
Erradicar y recuperar Incidente de Seguridad de la Información.			A/C	R
Documentar y adjuntar evidencias al caso creado en la herramienta de gestión			A/C	R
Validar y aprobar solución del Incidente de Seguridad de la Información			R	C
Documentar lecciones aprendidas en módulo de: Incidencias.		I	R	
Dar cierre al caso	I			R

R: Responsable de la correcta ejecución de la actividad.
A: Responsable por la calidad y resultados de la actividad.
C: Consultado (Brinda información o conocimiento)
I: Informado (recibe información sobre la ejecución o calidad de la actividad)

4. INDICADORES DE DESEMPEÑO

Indicador	Medición
% de Incidentes de Seguridad de la Información solucionados en el mes	(N° de incidentes de seguridad atendidos en el mes / Total de Incidentes de seguridad reportados en el mes) * 100

2. Disposiciones Generales

5. ENTRADAS Y SALIDAS DEL PROCEDIMIENTO

A continuación, se relacionan las diferentes entradas y salidas de la gestión de incidentes de los servicios de TI administrados por el operador:

Entradas del Procedimiento	Salidas del Procedimiento
• Reporte de eventos de seguridad de la información. • Reporte de Incidentes de seguridad de la información.	• Incidentes registrados, gestionados y solucionados. • Registro de lecciones aprendidas a través de módulo de Incidencias.

6. PROCEDIMIENTOS ASOCIADOS

Nombre del proceso	Descripción
Gestión de Incidentes	Al reportarse un incidente que impacte la confidencialidad, integridad, y/o disponibilidad de la información.
Gestión de Cambios	Al ejecutarse algún cambio dentro de los sistemas o aplicaciones del MEN que afecten la confidencialidad, integridad, y/o disponibilidad de la información.

7. DOCUMENTOS RELACIONADOS

- ST-AN-11 Flujograma - Procedimiento Gestión de Incidentes de Seguridad de la Información.
- ST-GU-14 Guía Política Gestión de Incidentes de Seguridad de la Información.
- ST-MA-04 Manual de Gestión de Incidentes de Seguridad de la Información.

3. Descriptivo del Procedimiento				
No.	**Descripción de actividades**	**Responsable**	**Tiempos**	**Evidencia**
1	**REPORTAR INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN** El reporte de Incidentes de Seguridad de la Información se realiza como resultado de las actividades de monitoreo de los servicios TIC, el análisis de vulnerabilidades que realiza la OTSI o por parte de los usuarios que los identifiquen o se vean afectados, a través de la Mesa de Ayuda y los canales de comunicación disponibles por el Ministerio: Línea telefónica, correo electrónico, Web (desde la página del Ministerio) e intranet. En los casos que el usuario desee que el reporte del Incidente sea anónimo, deberá contactar al responsable del SGSI en la OTSI, para que se guarde la confidencialidad sobre la identidad del usuario que reporta. Para lo cual, se debe enviar un correo a la cuenta: incidentessi@mineducacion.gov.co	Usuarios Internos y Externos MEN	Permanente	Herramienta de Gestión CA Service Desk Manager. Informes de Monitoreo y de análisis de vulnerabilidades.
2	**EVALUAR INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN** Analista de la Mesa de Ayuda evalúa el Incidente de Seguridad reportado de acuerdo a los tipos de incidentes descritos en el Manual de Gestión de Incidentes de Seguridad de la información ST-MA-04_V1.	Analista Mesa de Ayuda	0.0 hora 1 hora	Herramienta de Gestión CA Service Desk Manager.
3	**¿EVENTO REPORTADO CORRESPONDE A UN INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN?**	Analista Mesa de Ayuda		

3. Descriptivo del Procedimiento				
No.	**Descripción de actividades**	**Responsable**	**Tiempos**	**Evidencia**
	Según las habilidades y conocimientos del Analista de la Mesa de Ayuda se evalúa si el caso reportado corresponde a un Incidente de Seguridad de la Información. ¿Evento reportado corresponde a un Incidente de Seguridad de la Información? Si: Continuar en la actividad 5 No: Continuar en la actividad 4		0.0 hora 0.5 hora	Herramienta de Gestión CA Service Desk Manager.
4	**INTEGRACIÓN CON EL PROCEDIMIENTO GESTIÓN DE INCIDENTES** Envía el caso al procedimiento de gestión de incidentes para realizar atención del caso. Finaliza el procedimiento.	Analista Mesa de Ayuda	0.0 hora 0.5 hora	Herramienta de Gestión CA Service Desk Manager.
5	**CREAR, CATEGORIZAR Y PRIORIZAR EL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN** Analista de la Mesa de Ayuda crea, categoriza y prioriza el incidente de seguridad de la información según lo definido en el Manual de Gestión de Incidentes de Seguridad de la información ST-MA-04_V1.	Analista Mesa de Ayuda	0.5 hora 1 hora	Herramienta de Gestión CA Service Desk Manager.
6	**ESCALAR INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN AL RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN DE LA OTSI - MEN**	Analista Mesa de Ayuda	0.0 hora 0.5 hora	Herramienta de Gestión CA

3. Descriptivo del Procedimiento				
No.	**Descripción de actividades**	**Responsable**	**Tiempos**	**Evidencia**
	Analista de la Mesa de Ayuda escala el caso generado en la Herramienta de Gestión CA Service Desk Manager al responsable de seguridad de la información de la OTSI.			Service Desk Manager.
7	**ANALIZAR E IDENTIFICAR CASO ESCALADO** El responsable de Seguridad de la Información de la OTSI analiza e identifica si el caso escalado debe ser gestionado como un Incidente de Seguridad de la Información.	Responsable SI – OTSI-MEN	0.5 hora 1 hora	Herramienta de Gestión CA Service Desk Manager.
8	**¿CASO ESCALADO CORRESPONDE A UN INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN?** Según el conocimiento y la experiencia del responsable de Seguridad de la Información de la OTSI se evalúa si el caso escalado corresponde realmente a un Incidente de Seguridad de la Información. ¿Caso escalado corresponde a un Incidente de Seguridad de la Información? Si: Continuar en la actividad 9 No: Continuar en la actividad 4	Responsable SI – OTSI-MEN	0.0 hora 0.5 hora	Herramienta de Gestión CA Service Desk Manager.
9	**ESCALAR CASO AL GRUPO DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN PARA SU GESTIÓN** El responsable de Seguridad de la Información de la OTSI escala caso al Grupo de respuesta ante incidentes de seguridad de la información para que el mismo sea gestionado.		0.0 hora	Herramienta de Gestión CA

3. Descriptivo del Procedimiento				
No.	**Descripción de actividades**	**Responsable**	**Tiempos**	**Evidencia**
	El grupo de respuesta ante incidentes de seguridad de la información estará conformado por especialistas de los diferentes frentes del Operador de Servicios y especialistas de la OTSI del MEN quienes atenderán los casos según corresponda.	Responsable SI – OTSI-MEN	0.5 hora	Service Desk Manager.
10	**REALIZAR CONTENCIÓN DEL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN** El grupo de respuesta ante incidentes de seguridad de la información debe contener el impacto o efecto que el incidente puede llegar a tener dentro de los servicios tecnológicos del MEN. Para ello se deben identificar las causas del incidente y posteriormente se deben identificar las acciones correspondientes a aplicar y plantear los planes de mitigación de vulnerabilidades según aplique, lo anterior con la especificación de las fechas y responsables. En los casos que sea requerido de deberá activar el BCP (Plan de Continuidad del Negocio) o el DRP (Plan de Recuperación de Desastres) cuando el incidente de seguridad de la información afecte gravemente a un determinado activo de la información del MEN.	Grupo Respuesta a ISI-MEN	2 horas 4 horas	Herramienta de Gestión CA Service Desk Manager.
11	**¿SE LOGRO LA CONTENCIÓN DEL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN?**	Grupo Respuesta a ISI-MEN		

3. Descriptivo del Procedimiento				
No.	**Descripción de actividades**	**Responsable**	**Tiempos**	**Evidencia**
	El grupo de respuesta ante incidentes de seguridad de la información debe validar la contención del Incidente de Seguridad de la Información reportado. ¿Se logró la contención del Incidente de Seguridad de la Información? Si: Continuar en la actividad 12. No: Continuar en la actividad 10.		2 horas 4 horas	Herramienta de Gestión CA Service Desk Manager.
12	**ERRADICAR Y RECUPERAR INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN** El grupo de respuesta a incidentes de seguridad de la información debe ejecutar las acciones definidas dependiendo del tipo de incidente para erradicar y recuperar la información afectada, e informar el avance a las instancias o autoridades a quienes debe reportarse el incidente. Así mismo, debe brindar las recomendaciones necesarias para el tratamiento de nuevos incidentes como el reportado y de no poderse mitigar recomendar las acciones para su contención.	Grupo Respuesta a ISI-MEN	2 horas 4 horas	Herramienta de Gestión CA Service Desk Manager.
13	**¿SE LOGRO LA ERRADICACIÓN Y RECUPERACIÓN DEL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN?** El grupo de respuesta a incidentes de seguridad de la información debe informar si se logró la erradicación y recuperación del Incidente de Seguridad de la Información reportado.		2 horas 4 horas	Herramienta de Gestión CA

3. Descriptivo del Procedimiento				
No.	**Descripción de actividades**	**Responsable**	**Tiempos**	**Evidencia**
	¿Se logró la erradicación y recuperación del Incidente de Seguridad de la Información? Si: Continuar en la actividad 14. No: Continuar en la actividad 10.	Grupo Respuesta a ISI-MEN		Service Desk Manager.
14	**DOCUMENTAR Y ADJUNTAR EVIDENCIAS AL CASO EN LA HERRAMIENTA DE GESTIÓN** El grupo de respuesta a incidentes de seguridad de la información debe documentar y adjuntar todas las evidencias encontradas al caso que se generó en la herramienta de gestión para soportar la solución brindada al incidente presentado.	Grupo Respuesta a ISI-MEN	4 horas 7 días	Herramienta de Gestión CA Service Desk Manager.
15	**VALIDAR SOLUCIÓN Y APROBAR CIERRE DEL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN** El responsable de Seguridad de la Información de la OTSI debe validar si la solución brindada por el grupo de respuesta ante incidentes de seguridad de la información cumple con lo requerido para poder dar solución al incidente reportado.	Responsable SI – OTSI-MEN	4 horas 7 días	Herramienta de Gestión CA Service Desk Manager.
16	**¿SE APRUEBA SOLUCIÓN DEL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN?** El responsable de Seguridad de la Información de la OTSI debe aprobar la solución brindada al incidente de seguridad de la información. ¿Se aprueba solución del incidente de seguridad de la información?	Responsable SI – OTSI-MEN	4 horas 7 días	Herramienta de Gestión CA Service Desk Manager.

3. Descriptivo del Procedimiento				
No.	**Descripción de actividades**	**Responsable**	**Tiempos**	**Evidencia**
	Si: Continuar en la actividad 17. No: Continuar en la actividad 14.			
17	**DOCUMENTAR LECCIONES APRENDIDAS EN MODULO DE INCIDENCIAS** El responsable de Seguridad de la Información de la OTSI a través del Módulo de Incidencias habilitado en la herramienta de gestión debe documentar las lecciones aprendidas una vez solucionado el incidente de seguridad de la información.	Responsable SI – OTSI-MEN	4 horas 7 días	Herramienta de Gestión CA Service Desk Manager.
18	**DAR CIERRE AL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN** Una vez se cuente con el visto bueno del responsable de Seguridad de la Información de la OTSI el grupo de respuesta ante incidentes de seguridad de la información podrá proceder a solucionar el caso reportado a través de la herramienta de gestión. **Finaliza Procedimiento**	Grupo Respuesta a ISI-MEN	4 horas 7 días	Herramienta de Gestión CA Service Desk Manager.

4. Control de Cambios		
Versión	**Fecha de entrada en vigencia**	**Naturaleza del cambio**

01	Rige a partir de su publicación en el SIG	Se crea procedimiento para el adecuado manejo y reporte de los Incidentes de Seguridad de la Información en el Ministerio de Educación Nacional con el fin de proteger la Confidencialidad, Integridad y Disponibilidad de sus activos de información los cuales incluyen (hardware, software y su todo su personal).

5. Ruta de aprobación					
Elaboró		**Revisó**		**Aprobó**	
Nombre	Edwar Aldemar Hidalgo	**Nombre**	Lina Vannesa Perdomo Castrillón	**Nombre**	Roger Quirama García
Cargo	Contratista Oficina de Tecnología y Sistemas de Información	**Cargo**	Contratista Subdirección de Desarrollo Organizacional	**Cargo**	Jefe de Oficina de Tecnología y Sistemas de Información