1. PROPOSITO

Minimizar, controlar, reportar y responder de manera oportuna y apropiada ante un impacto de un incidente de seguridad de la información presentados en la Alcaldía Mayor de Cartagena de Indias.

2. ALCANCE

Aplica a la gestión de todos los eventos e Incidentes de seguridad de la Información al interior de la Alcaldía Mayor de Cartagena de Indias, desde la apertura de la incidencia hasta el cierre de esta.

3. GLOSARIO

- **Incidente:** Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una política de seguridad o de tratamiento de la información.
- **Falsa Alarma:** Reporte de evento que no cumple con la característica de afectación de la Confidencialidad, Integridad y Disponibilidad de la Información.
- **Suplantación de identidad:** Todas aquellas actividades realizadas por la que una persona se hace pasar por otra para llevar a cabo actividades de carácter ilegal.
- **Ingeniería social** es una de las formas en las que los cibercriminales usan las interacciones entre personas para que el usuario comparta información confidencial. Ya que la ingeniería social se basa en la naturaleza y las reacciones humanas, hay muchas formas en que los atacantes pueden engañar, en línea o sin conexión.

- **Spam:** es cualquier forma de comunicación no solicitada que se envía de forma masiva (correo electrónico masivo no solicitado, o UBE). Su forma más frecuente es un correo electrónico de publicidad enviado a un gran número de direcciones (correo electrónico de publicidad no solicitado, o UCE), pero el "spamming" también existe a través de menajes instantáneos, de texto (SMS), redes sociales o incluso mensajes de voz. Enviar spam es ilegal en la mayoría de las jurisdicciones.
- **Integridad:** Propiedad de la información relativa a su exactitud y completitud.
- **Confidencialidad:** Propiedad de la información restringe su disposición o revelación a individuos, entidades o procesos no autorizados.
- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera un individuo, entidad o procesos autorizados.

4. RESPONSABILIDAD Y AUTORIDAD

- **Gestor de Seguridad** es el responsable de planificar, desarrollar, controlar, gestionar y/o coordinar las estrategias de seguridad de la información, con el fin de mantener la confidencialidad, integridad y disponibilidad; y de promover el diseño, establecimiento, implementación, operación, revisión, mantenimiento y mejora continua de la gestión en seguridad de la información. Descritas en el anexo 1 categorización de plataforma SAUS
- **Especialista de Seguridad** es el responsable de la gestión y administración de la infraestructura de seguridad informática, gestionar la remediación de vulnerabilidades técnicas y monitorear los eventos de seguridad de la infraestructura tecnológica, así como coordinar las acciones de respuesta y recuperación al incidente se seguridad de la información.
- **Mesa de Servicio** Recibe la información de los funcionarios - Contratistas de la Alcaldía Mayor de Cartagena de Indias, registra los casos en la

herramienta SAUS y es el primer contacto para la gestión de los incidentes de seguridad.

5. (POLITICAS DE OPERACIÓN) CONSIDERACIONES GENERALES

Para la gestión de incidentes en necesario analizar y tener presente las siguientes consideraciones generales:

- **Política de comunicaciones y notificación del Incidente**

Todo incidente de seguridad que afecte la infraestructura del Distrito debe ser notificado en tiempo real ante el equipo de respuesta a incidentes de seguridad de la información, conformado por el responsable de Seguridad de la Información, Administradores de los Sistemas de Información, Director del jefe de la oficina asesora de Informática , Técnico de Mantenimiento, subproceso de infraestructura de acuerdo con lo establecido en el instructivo para la definición de roles y responsabilidades del modelo de seguridad y privacidad de la información GTIGPS01-I002.

Se deberá reportar por el encargado de Seguridad Digital todos los incidentes cibernéticos. Una vez se reciba el reporte del posible Incidente de seguridad, el gestor de seguridad deberá realizar la primera categorización, para iniciar con la atención de este; si cumple con algunos de los siguientes criterios puede ser considerado como un incidente de seguridad, de lo contrario se tratará como un evento:

- Hubo daño, fuga, robo o pérdida de información física o digital.
- Hubo robo de credencias o información mediante Phishing.
- Se presentó modificación no autorizada de la información.
- Se presentó suplantación de identidad.
- Se presentó un acceso no autorizado.
- Se presentó pérdida o alteración de registros de base de datos o SQL injection.
- Se presentó una pérdida de un activo de información.
- Hubo presencia de código malicioso “malware”.
- Se presentó una denegación del servicio.
- Se presentó algún ciberataque.

Posterior a que un incidente se haya analizado y priorizado se debe notificar al personal encargado de la gestión y atención de incidentes y a las entidades que

determine el líder de la oficina asesora de informática.

- Las personas que deben ser notificadas cuando ocurra un incidente teniendo en cuenta el nivel de impacto, son las siguientes:

Cargo	Medio de contacto
Líder del equipo de seguridad	Seguridad.oai@cartagena.gov.co
Mesa de servicios (administradores de la infraestructura TI)	Correo institucional de la mesa de servicios soportegti@cartagena,gov.co Línea de Atención telefónica: 3023798584
Jefe de la oficina Asesora de informática	informatica@cartagena.gov.co
Mesa de servicio CSIRT Gobierno	018000910742, Opción 2, seguridad digital. csirtgob@mintic.gov.co
Superintendencia de industria y comercio	Contact center+57 (601) 592 0400 Bogotá - Línea Gratuita Nacional: 01 8000 910165 Teléfono Conmutador: +57 (601) 587 0000 - Bogotá Correo Institucional: contactenos@sic.gov.co
Equipo de atención de incidentes de la policía Nacional	Teléfonos: (571) 5159090 / 5159586 Email: ponal.csirt@policia.gov.co
Equipo de atención de incidentes del Ministerio de defensa	Colcert.gov.co
Oficina de control disciplinario	controldisciplinario@cartagena.gov.co
Oficina de talento humano	talentohumano@cartagena.gov.co
Unidad de delitos informáticos de la fiscalía general de la nación	01 8000 9197 48 o desde celular al 122, Ventanilla única de correspondencia Calle 66 No. 4-86 Barrio Crespo Cel 3165210785 – Fijo 6056694330

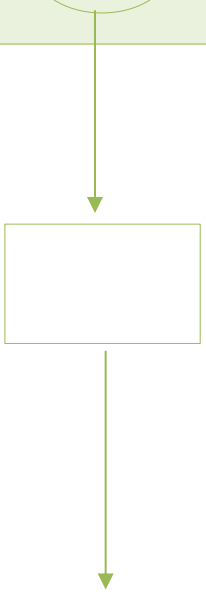
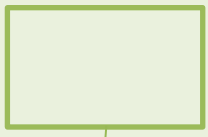
- **Documentos para el reporte**

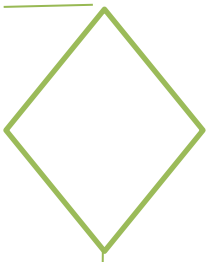
A continuación, encontrará una serie de documentos y formularios que deben ser diligenciados de acuerdo con el evento o incidente presentado:

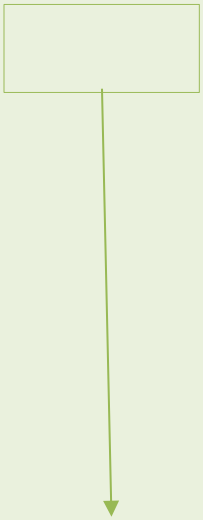
- Crear caso en la mesa de servicio de la Alcaldía a través de la plataforma SAUS y adjuntar el Formato Reporte de Incidentes.

- Una vez creado el caso, reenviar dicha información al área de seguridad y privacidad por medio del correo Seguridadoai@cartagena.gov.co con copia a informatica@cartagena.gov.co
-

6. DESCRIPCIÓN DE TAREAS

No.	SIMBOLO FLUJOGRAMA	TAREA	DESCRIPCIÓN	RESONSABLE	REGISTRO
1		Inicio	Inicio del procedimiento		
2		Reportar	Todos los funcionarios, contratistas y/o terceros deben reportar cualquier evento y/o incidente de seguridad de la información, a través de los siguientes canales: • Correo institucional de la mesa de servicios soportegti@cartagena,gov.co • Línea de Atención telefónica: 3023798584. • Sigob. Sin excepción, sea cual sea el medio por el cual se reportó el evento y/o incidente de Seguridad de la Información, deben quedar registradas en la herramienta de gestión SAUS.	Funcionarios / Contratistas Mesa de Servicios y Terceros	Reporte en la plataforma SAUS Correo electrónico SIGOB
3		Categorizar y Registrar	La Mesa de Servicios recibe el reporte del evento y/o incidente de seguridad de Seguridad de la Información, lo identifica, registra, clasifica y escala inmediatamente al el Gestor de Seguridad de Seguridad Informática responsable.	Funcionarios / Contratistas Mesa de Servicios	Reporte del incidente
	  	Recolectar Información	El Gestor de Seguridad debe realizar la evaluación inicial que involucra el análisis de la información descrita en el reporte e información adjuntada por la Mesa de Servicios, si existe. En caso de no existir la información suficiente para la evaluación del hallazgo el Asesor/Especialista de	Gestor de Seguridad / Área de Seguridad	Reporte de la información en SAUS Formato reporte de incidentes de seguridad (formato de

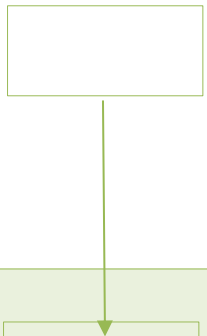
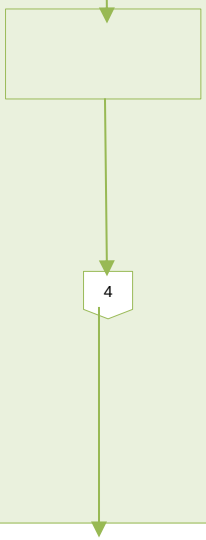
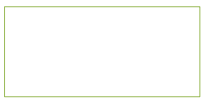
4	No  Si 2		Seguridad debe establecer comunicación con el personal involucrado para así recolectar la información necesaria que permita precisar la clasificación del reporte. El reporte puede ser clasificado en: ✓ Malware ✓ Disponibilidad ✓ Obtención de Información: ✓ Intrusiones: . ✓ Compromiso de Información: . ✓ Fraude: ✓ Contenido Abusivo: ✓ Política de Seguridad: Son catalogados incidentes de seguridad de la información los que coincidan con las siguientes causas: - Ejecución de Denegación de Servicio. - Hacking. - Ejecución de Pruebas Maliciosas o Escaneos de Red. - Contraseñas comprometidas. - Llaves de cifrado comprometidas. - Suplantación de sitios Web Phishing. - Suplantación de identidad de funcionarios. - Introducción de código malicioso (Virus, gusanos, troyanos) - Ingeniería social. - Distribución de spam. - Acceso no autorizado a sistemas de información o redes. - Cambio de privilegios sobre sistemas de información sin autorización. - Modificación o inserción de transacciones, archivos o bases de datos sin autorización. - Descarga o envió de contenido inapropiado. - Divulgación no autorizada de información del negocio. - Piratería de software. - Robo de información de negocio.		origen externo)

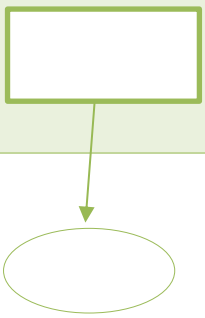
			- Robo de información personal de clientes y/o funcionarios (ej.: Phishing). - Pérdida o hurto de equipo de cómputo. - Robo de software. - Robo de información de autenticación. - Daño o pérdida de los servicios o enlaces de comunicaciones. Una vez diligenciado el formato se adjunta al reporte realizado en la plataforma SAUS, para su trazabilidad. Si el reporte corresponde a una falsa alarma, se debe documentar en SAUS la justificación de la decisión y posteriormente se debe cerrar y notificar a los interesados.		
5		Análisis y Evaluación del Impacto	El Gestor de Seguridad de la Información debe determinar: - Valorar el Impacto (Confidencialidad e Integridad). - Valorar la Urgencia (Disponibilidad). - Determinar de la Prioridad (Impacto * Urgencia). - Afectación. - Causas o Tipo de Ataque. Adicionalmente, el Gestor de Seguridad debe informar al Asesor/Especialista de Seguridad Informática para planear las actividades enfocadas a contener, controlar y restaurar a la normalidad las operaciones afectadas por el incidente, esto mediante las siguientes tareas, las cuales deben ser documentadas en el sistema, las acciones pueden ser: La criticidad para clasificarla en función de su impacto, y establecer el nivel de prioridad en la resolución de cada incidente de Seguridad de la Información. Se categorizan las	Gestor de Seguridad	Formato informe de incidentes de seguridad

			incidencias en los siguientes términos: - Critica. - Grave. - Moderada. - Leve - Acciones de contención (Si se requieren). - Acciones complementarias (Si se requieren). Esta información se deberá diligenciar de acuerdo con el instructivo para realizar informes de incidentes de seguridad.		
6		Aplicar acciones de contención	El Asesor/Especialista de Seguridad Informática si aplica, debe identificar las acciones de respuesta inmediata (Contención) con el Área de Infraestructura TI para tratar el incidente, esto puede dar como resultado controles de Emergencia y/o controles permanentes adicionales. El plan de acción puede contener acciones como: - Activar Contingencias - Desconectar - Copiar/Clonar - Registrar posibles evidencias - Establecer posibles causas - Notificar a los interesados El Asesor/Especialista de Seguridad Informática gestiona la ejecución de las actividades del plan de acción enfocadas en la recuperación de la operación. Dentro de estas actividades pueden estar: - Ejecución de las acciones de restauración - Implantación de medidas de remediación - Pruebas - Ejecución de plan de retorno Cualquiera que sea el resultado de las acciones realizadas, se debe	Gestor de Seguridad	Formato de informe de incidentes de seguridad

			hacer seguimiento a las acciones por parte del Gestor de Seguridad de la información verificando la documentación y evidencias registradas. Una vez finalizada las acciones de contención, el Gestor de Seguridad determina si el incidente de Seguridad de la Información está bajo control. Una vez finalizada las acciones de contención, el Gestor de Seguridad determina si el incidente de Seguridad de la Información está bajo control.		
7		**Reportar incidentes de seguridad a los entes externos**	El Gestor de seguridad de acuerdo con el análisis realizado determina si el impacto del incidente de seguridad es enviado a los entes externos. Se pueden reportar incidentes de seguridad de la información a través de los siguientes canales, de lo contrario se maneja el incidente interno en la Entidad. • **Reporte de Incidentes** Identificado el incidente cibernético, por el encargado de seguridad digital en el Distrito, se debe diligenciar el formato de reporte de incidentes en su totalidad y enviarlo al CSIRT Gobierno para su gestión y acompañamiento. • **Mesa de servicio CSIRT Gobierno** Contactando a la mesa de servicio, llamando a la línea gratuita 018000910742, Opción 2, seguridad digital. • **Correo electrónico:** Enviando un mensaje de correo electrónico informando el incidente al buzón csirtgob@mintic.gov.co,	Gestor de seguridad / Área de Seguridad	Formato informe de seguridad de la información Correo electrónico

			adjuntando el Formato de Reporte de Incidentes debidamente diligenciado. el Gestor de seguridad, será el punto de contacto con dicha entidad durante todo el proceso hasta que se dé la solución a la incidencia. • **ColCERT:** (Grupo de Respuesta a Emergencias Cibernéticas de Colombia), reportar al correo electrónico: contacto@colcert.gov.co o al Teléfono: (+571) 2959897. **Centro cibernético Policial** reportar en la siguiente ruta: https://caivirtual.policia.gov.co/		
8		Aplicar acciones Complementarias	El Asesor/Especialista de Seguridad Informática con el equipo especialista del sistema de información debe identificar si se requieren actividades complementarias para tratar los incidentes de seguridad de la información, esto puede incluir la restauración del Sistema(s), Servicio(s) y/o redes de información a su estado normal.	Asesor/Especialista de Seguridad Informática / equipo especialista del sistema de información	Formato informe de seguridad de la información
9	4	Notificar	El Asesor/Especialista de Seguridad Informática, almacena copia de las evidencias recopiladas en el repositorio destinado para este fin, con las debidas restricciones al acceso por ser información sensible, y documenta el incidente por medio de la plataforma SAUS. La información que debe contener como mínimo es: - Fecha de Solicitud. - Persona que lo diligencia. - Ubicación. - Descripción del incidente (descripción cronológica de los acontecimientos). - Clasificación del incidente de acuerdo con el procedimiento (en	Asesor/Especialista de Seguridad Informática	Formato informe de seguridad de la información Plataforma SAUS

			caso de que el evento sí sea incidente). - Posibles Impactos. - Partes involucradas (especificar especialmente si hay terceros involucrados). - Acciones realizadas (Medidas de contención y de recuperación).		
10		Comunicación a los afectados	Una vez identificado el incidente de seguridad y cumplidas con las actividades descritas en el presente procedimiento, la Oficina Asesora de Informática comunicara al interesado en un lenguaje claro y sencillo la violación de seguridad, las medidas correctivas adoptadas por la organización y las recomendaciones de seguridad que deberán seguir los interesados.	Funcionarios de la OAI	Sigob Correo electrónico
11		Documentar Lecciones Aprendidas	El Gestor de Seguridad con el equipo que atendiendo el incidente es responsable de identificar las lecciones aprendidas con el objeto de evitar la reincidencia de los hechos y la eliminación de las debilidades aprovechadas por la amenaza que causó el incidente de seguridad. Así mismo, el Gestor de Seguridad de la Información es responsable de identificar si aplica, controles nuevos o modificaciones a los existentes en la Alcaldía Mayor de Cartagena de Indias, esto en Pro de mejorar el proceso y la Seguridad de la Información de la Alcaldía Mayor de Cartagena de Indias.	Gestor de Seguridad / Área de Seguridad	Informe de incidente de seguridad
12		Cerrar El incidente	El Gestor de Seguridad con el equipo que atendiendo el incidente es responsable de identificar las lecciones aprendidas con el objeto de evitar la reincidencia de los hechos y la eliminación de las debilidades aprovechadas por la amenaza que causó el incidente de seguridad. Así mismo, el Gestor de Seguridad de la Información es responsable de identificar si aplica, controles nuevos	Gestor de Seguridad	Informe de incidente de seguridad

			o modificaciones a los existentes en la Alcaldía Mayor de Cartagena de Indias, esto en Pro de mejorar el proceso y la Seguridad de la Información de la Alcaldía Mayor de Cartagena de Indias		
		Cerrar el incidente	El Gestor de Seguridad informa a la Mesa de Servicios de la Oficina Asesora de Informática para el cierre del incidente en la herramienta de gestión e informa a las personas interesadas.	Gestor de Seguridad	Informe de Cierre del incidente
13		Fin	Fin del procedimiento		

7. DOCUMENTOS DE REFERENCIA:

Guía para la gestión de incidentes MINTIC

8. CONTROL DE CAMBIOS

FECHA	DESCRICPCION DE CAMBIOS	VERSION
28/06/2023	**Elaboración del documento**	**1.0**
04/10/2023	**Se aclaran las políticas de comunicación de incidentes de seguridad**	**2.0**

9. VALIDACION DEL DOCUMENTO

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre: Jhonattan Bawin Romero **Nombre: Carlos Gómez** **Cargo: Asesor Externo** **Fecha: 04/10/2023**	**Nombre: Jasmin Herrera** **Cargo: Asesor externo** **Fecha: 04/10/2023**	**Nombre: Ingrid Solano** **Cargo: jefe Oficina Asesora de informática** **Fecha: 04/10/2023**