PROCEDIMIENTO

GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

CUADRO DE CONTROL

ELABORÓ	REVISO	APROBÓ
FUNDACIÓN PACÍFICO ATLÁNTICO	Funcionario Responsable Enlace	Director TICS ANDRÉS SANTIAGO VALENCIA HINCAPIÉ Representante Alta Dirección

CONTROL DE CAMBIOS

VERSION	ORIGEN DE LOS CAMBIOS	FECHA DE REGISTRO			NOMBRE DEL FUNCIONARIO
		DIA	M ES	AÑO	
1	Creación del Procedimiento	17	04	2023	FUNDACION PACIFICO ATLANTICO

1. OBJETIVO

Garantizar la atención de los incidentes que se presenten en los activos de información del municipio de Cartago y que atenten contra sus características de confidencialidad, integridad y Disponibilidad, así como la atención eficaz y oportuna de los mismos.

2. ALCANCE

Este procedimiento inicia con la notificación del incidente al comité de seguridad y privacidad de la información de acuerdo con el formato de reporte de incidentes, termina con su correcta gestión y tramite.

3. MARCO LEGAL

Ley 23 de 1982: “Sobre derechos de autor”

Ley 603 de 2000: “Por la cual se modifica el artículo 47 de la Ley 222 de 1995”

Ley 1564 de 2012: “Por medio de la cual se expide el Código General del Proceso y se dictan otras disposiciones”

Decreto 1008 de 2018: “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la información y las Comunicaciones”

Norma ISO 27001: ISO 27001 es una norma desarrollada por ISO (organización internacional de Normalización) con el propósito de ayudar a gestionar la Seguridad de la Información en una empresa.

4. DEFINICIONES

Actualización: Una nueva versión de un programa informático o equipo diseñada para reemplazar a una antigua versión del mismo producto. Generalmente, las empresas de software venden actualizaciones a precios de descuento. En la mayoría de los casos, usted debe probar que posee una versión anterior del producto para beneficiarse con el precio de actualización.

Incidente de seguridad en informática: Es la ocurrencia de uno o varios eventos que atentan contra la confidencialidad, la integridad y la disponibilidad de la información y que violan la Política de Seguridad de la Información de la organización, en el caso de que disponga de ella.

Licencia: Permiso de uso parcial o total de un programa o porción de este para uso con o sin lucro.

Requerimiento Técnico: Aviso o manifestación de una situación problema a nivel técnico.

Seguridad informática: Cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática cuyos efectos puedan conllevar daños sobre la información, equipo o software.

Software: programas que ejecutan ciertas tareas en un computador, permite realizar tareas de todo tipo. Desde mandar un correo a gestionar la contabilidad de una empresa. Las aplicaciones son parte del software de una computadora y suelen ejecutarse sobre el sistema operativo.

Tecnologías de la información y las comunicaciones (TICS): Son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes.

Usuario final: El usuario final o último de un producto y/o sistema informático.

Versión: Hace referencia al modelo de programa que se está usando se usa para saber si el programa está o no actualizado con los últimos cambios hechos por el fabricante.

5. RESPONSABLE

Es responsabilidad del Director TICS, la gestión de las actividades propuestas en este procedimiento, para el logro de los objetivos trazados.

6. POLITICAS DE OPERACIÓN

- Todos los registros que se generen en el procedimiento deben ser archivados de acuerdo con lo definido en la tabla de retención documental (TRD), teniendo en cuenta los lineamientos de los instrumentos archivísticos y la ley 594 de 2000 sobre los Archivos de gestión.

- La atención al ciudadano será justa y equitativa, no existirán prelaciones en la atención ni discriminaciones por credo, raza; inclinación política, religiosa, ni económica.

- Cuando se presenten peticiones, quejas o reclamos anónimos o que no indiquen dirección para remisión de correspondencia o dirección electrónica, se publicara la respuesta en la página Web oficial del municipio www.municipiodecartago.gov.co y en la cartelera oficial de la misma Secretaría, por un término de diez (10) días hábiles.

- Cualquier problema que ocurra con los equipos tecnológicos deberá ser reportado al responsable de su dependencia o en su defecto a la Dirección TICS del Municipio.

- Se establece que los únicos autorizados para firmar las comunicaciones oficiales son el Alcalde, Secretarios(as) de Despacho y los (las) delegados(as) que se encuentren autorizados en el manual o Decreto de firmas del Municipio.

- Cuando se presente un posible evento de seguridad de información se debe reportar al comité de seguridad y privacidad de la información mediante los siguientes pasos:

1. Solicitud del jefe inmediato mediante memorando, donde se anexe el formato de reporte de incidentes de seguridad de la información.
2. Clasificación del incidente de acuerdo con los parámetros de seguridad.
3. Tratamiento del incidente de acuerdo con la clasificación, conocimiento de la gravedad y el tiempo acordado para su atención. (El tratamiento se determina de acuerdo con el documento estrategia de resolución de incidentes de seguridad de la información).
4. Una vez se resuelve el incidente, se registra toda la información generada durante el tratamiento en una base de datos de conocimiento y se envía la notificación de cierre del incidente a la persona que envió la notificación.

- Para el caso de la atención de incidentes de seguridad se ha establecido unos tiempos máximos de atención de estos, con el fin de atender adecuadamente los incidentes de acuerdo con su criticidad e impacto. Los tiempos expresados en la siguiente Tabla son un acercamiento al tiempo máximo en que el incidente debe ser atendido, ***y no al tiempo en el cual el incidente debe ser solucionado***. Esto se debe a que la solución de los incidentes puede variar dependiendo del caso.

7. CONTENIDO Y DESARROLLO

Inicio: Se da inicio al procedimiento **GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA**, teniendo en cuenta el cumplimiento legal vigente.

Recibir la notificación del incidente: Recibir el memorando del Jefe de Oficina donde se notifica el incidente el cual debe llevar anexo el formato de incidentes de seguridad de la información.

Clasificar el incidente de seguridad de la información: Se procede a clasificar el incidente estableciendo si es una amenaza o no lo es. En caso de ser un incidente de seguridad se clasifica de acuerdo con el tipo de incidente, y se prioriza de acuerdo con el nivel de criticidad e impacto.

CLASIFICACIÓN DE LOS INCIDENTES	
Acceso no autorizado	Es un incidente que involucra a una persona, sistema o código malicioso que obtiene acceso lógico o físico sin autorización adecuada del dueño a un sistema, aplicación, información o un activo de información.
Modificación de recursos no autorizado	Un incidente que involucra a una persona, sistema o código malicioso que afecta la integridad de la información o de un sistema de procesamiento.
Uso inapropiado de recursos	Un incidente que involucra a una persona que viola alguna política de uso de recursos.
No disponibilidad de los recursos	Un incidente que involucra a una persona, sistema o código malicioso que impide el uso autorizado de un activo de información.
Multicomponente	Un incidente que involucra más de una categoría anteriormente mencionada.
Otros	Un incidente que no puede clasificarse en alguna de las categorías anteriores. Este tipo de incidentes debe monitorearse con el fin de identificar la necesidad de crear nuevas categorías.

- **Nivel de prioridad.**

Establece el nivel de atención adecuada del incidente para que de esta manera se atienda adecuadamente según la necesidad.

El nivel de prioridad se establece de acuerdo con la siguiente formula:

Nivel de Prioridad: (Impacto Actual * 2,5) + (Impacto Futuro * 2,5) + (Criticidad del Sistema * 5)

Nivel de Impacto (Actual o Futuro)	Valor	Definición
Inferior	**0,10**	Impacto leve en uno de los componentes de cualquier sistema de información o estación de trabajo
Bajo	**0,25**	Impacto moderado en uno de los componentes de cualquier sistema de información o estación de trabajo. Medio
Medio	**0,50**	Impacto alto en uno de los componentes de cualquier sistema de información o estación de trabajo
Alto	**0,75**	Impacto moderado en uno o más componentes de más de un sistema de información
Superior	**1,00**	Impacto alto en uno o más componentes de más de un sistema de información.

Nivel de Criticidad	Valor	Definición
Inferior	**0,10**	Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas
Bajo	**0,25**	Sistemas que apoyan a una sola dependencia o proceso de una entidad
Medio	**0,50**	Sistemas que apoyan más de una dependencias o proceso de la entidad
Alto	**0,75**	Sistemas pertenecientes al área de Tecnología y estaciones de trabajo de usuarios con funciones críticas.
Superior	**1,00**	Sistemas Críticos

Nivel de Prioridad del Incidente	Valor
Inferior	00,00 – 02,49
Bajo	02,50 – 03,74
Medio	03,75 – 04,99
Alto	05,00 – 07,49
Superior	07,50 – 10,00

Tratamiento del incidente de acuerdo con la clasificación: De acuerdo con la clasificación se implementa una estrategia que permita tomar decisiones oportunas para evitar la propagación del incidente y así disminuir los daños a los recursos de TI.

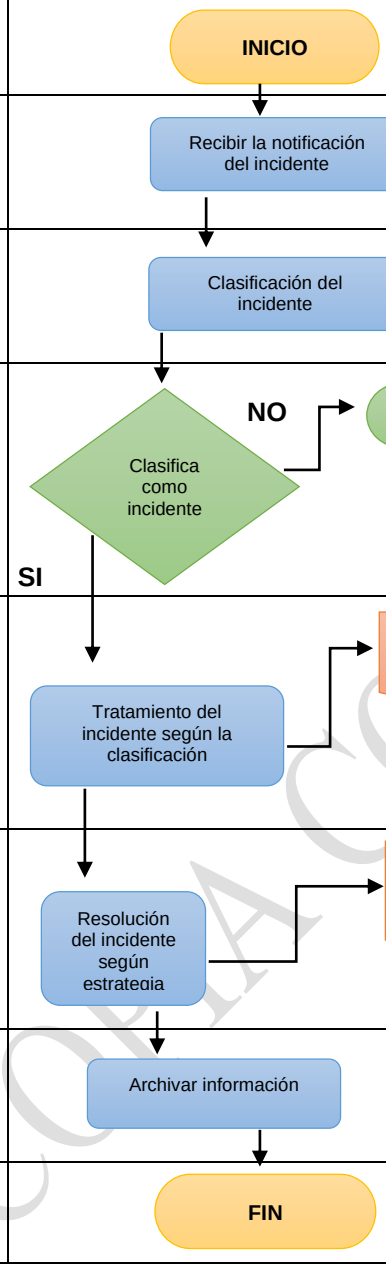
Resolución del incidente: De acuerdo con la estrategia implementada se registran todas las actividades de resolución en una base de datos de conocimiento y se envía memorando de notificación con el cierre del incidente de seguridad de la información.

TIEMPOS DE RESPUESTA	
Nivel de Prioridad	**Tiempo de Respuesta**
Inferior	24 horas
Bajo	12 horas
Medio	6 horas
Alto	1 hora
Superior	30 min

Archivo: Remitirse al procedimiento de gestión documental.

Fin: Da terminación a las actividades propias del procedimiento **GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA.**

7.1 Flujo grama del procedimiento

No.	ACTIVIDAD	RESPONSABLE	REGISTRO
			
1		Director TICS	*Memorando *Formato diligenciado
2		Comité de Seguridad y Privacidad de la información	Registro de comité
3		Comité de Seguridad y Privacidad de la información	Registro de comité
4		Comité de Seguridad y Privacidad de la información	*Estrategia implementada *Resolución de incidente
		Comité de Seguridad y Privacidad de la información	Acta de actividades de resolución de incidente
5		Técnico administrativo	Archivo físico y digital

8. RIESGOS VS CONTROLES

Ver Mapa de Riesgos

9. CONTROL DE DOCUMENTOS Y REGISTROS

Ver Listado Maestro de Documentos
Ver Tabla de Retención Documental