PROCEDIMIENTO

GESTIÓN DE RIESGOS 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

Establecer la metodología para gestionar el riesgo en la entidad, que incluye su identificación, análisis, evaluación, tratamiento con el fin de prevenir o reducir el impacto de un incidente en la seguridad de la información.

2. ALCANCE

Este procedimiento inicia con la identificación, clasificación, análisis y evaluación de los riesgos de seguridad de la información hasta el control y valoración de estos.

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

Activo de Información: Según la norma ISO 27000:2013 un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección.

Amenaza: Es todo aquello que tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la entidad.

Gestión del Riesgo: Actividades coordinadas para dirigir y controlar una entidad con respecto al riesgo.

Riesgo: Es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso de la entidad.

Riesgos de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

Riesgo Estratégico: Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

Riesgos de Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.

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.

Vulnerabilidad: Es una debilidad que puede permitir que se materialice una amenaza sobre el activo de información.

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.

7. CONTENIDO Y DESARROLLO

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

Establecer el contexto Estratégico: Desarrollar un análisis de Debilidades, Oportunidades, Fortalezas y Amenazas para cada uno de los procesos o activos de información con clasificación ALTA en cuanto a los criterios de clasificación para integridad, confiabilidad y disponibilidad.

Identificar Riesgos: De acuerdo con la Matriz DOFA, se procede a clasificar por clase de riesgos estratégicos, operativos, financieros, normativos, tecnológicos, de conocimiento una lista de eventos que probablemente logren que una amenaza se materialice.

Analizar Riesgos: En esta etapa con la identificación del riesgo, se establecen las amenazas, las vulnerabilidades y las consecuencias que se puedan presentar si el riesgo se materializa.

Evaluación de los Riesgos: De acuerdo con las etapas anteriores de identificación y análisis se procede a cuantificar la probabilidad de ocurrencia y el impacto de sus consecuencias de acuerdo con los criterios de riesgo del presente documento, procediendo a calcular el nivel de riesgo, que es el producto de multiplicar las calificaciones de la probabilidad y el impacto.

Para medir la probabilidad de que determina que un evento ocurra se va a emplear lasiguiente escala.

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.
2	Improbable	El evento puede ocurrir en algún momento	Al menos de 1 vez en losúltimos 5 años.
3	Posible	El evento podría ocurrir en algún momento	Al menos de 1 vez en losúltimos 2 años.
4	Probable	El evento probablemente ocurrirá en la mayoríade las circunstancias	Al menos de 1 vez en elúltimo año.
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año.

Para medir el impacto que tendrá un evento en la entidad se va a emplear lasiguiente escala.

NIVEL	DESCRIPTOR	DESCRIPCIÓN
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

De acuerdo con la cuantificación de la probabilidad de ocurrencia de un evento y el grado de severidad de sus consecuencias en los objetivos institucionales o de proceso, se establece el nivel de riesgo, el cual es producto de la aplicación de la siguiente formula:

NIVEL DE RIESGO= PROBABILIDAD X IMPACTO

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	1	2	3	4	5
Improbable (2)	2	4	6	8	10
Posible (3)	3	6	9	12	15
Probable (4)	4	8	12	16	20
Casi Seguro (5)	5	10	15	20	25

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

ZONA DE RIESGO	
	BAJO (B)
	MODERADO (M)
	ALTO (A)
	EXTREMO (E)

Valoración del Tratamiento del Riesgo: De acuerdo con los riesgos se escogen los controles o se crean nuevos que permitan disminuir la exposición del riesgo, y luego se debe hacer un recalculo comparando nuevamente con los criterios establecidos y así buscar un nivel aceptable del riesgo en cada proceso para los temas de Seguridad.

Plan de Implementación: De acuerdo con los Controles elegidos que permitirán minimizar el riesgo, se establece un plan de implementación de riesgo de seguridad de la información.

Opciones de manejo sugeridas de acuerdo con el nivel del riesgo establecido.

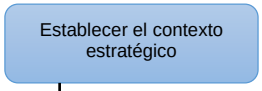
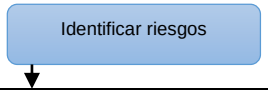
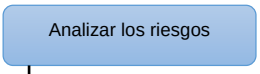
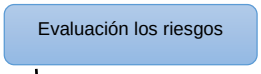
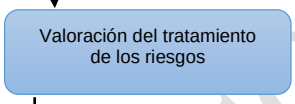
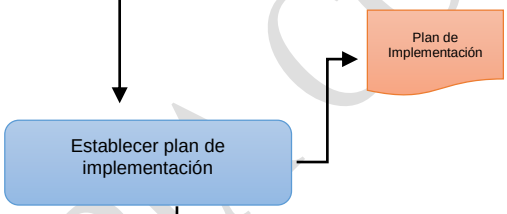
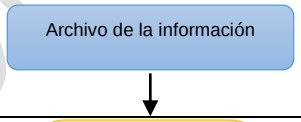
ZONA DE RIESGO		OPCIONES DE MANEJO
	BAJO (B)	• Asumir el riesgo
	MODERADO (M)	• Asumir el riesgo • Reducir el riesgo
	ALTO (A)	• Reducir el riesgo • Evitar el riesgo • Compartir o transferir
	EXTREMO (E)	• Evitar el riesgo • Reducir el riesgo • Compartir o transferir

- Asumir el riesgo: en riesgos de nivel bajo o moderado se hace mediante una decisión informada pueden mantener los controles ya establecidos.
- Reducir el riesgo: tomando acciones para reducir la probabilidad de ocurrencia y/o los efectos de sus consecuencias.
- Evitar el riesgo: retirando la fuente del riesgo o decidiendo no iniciar o continuar la actividad que lo origino.
- Compartir el riesgo: se hace mediante suscripción de pólizas, o transfiriendo el riesgos a otras partes (contractual), o mediante la transferencia física a otros lugares (ejemplo:transferir a un tercero la protección y custodia de activos de información – archivos de seguridad).
- Asumir el riesgo para perseguir una oportunidad, en este caso se elabora un plan de tratamiento del riesgo con las opciones antes enunciadas.

Archivo: Remitirse al procedimiento de gestión documental.

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

7.1 Flujograma del procedimiento

No.	ACTIVIDAD	RESPONSABLE	REGISTRO
			
1		Director TICS	Matriz DOFA
2		Director TICS	Matriz de riesgos
3		Director TICS	Matriz de riesgos
4		Director TICS	Matriz de riesgos
5		Director TICS	Matriz de riesgos
6		Director TICS	Plan de implementación
7		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