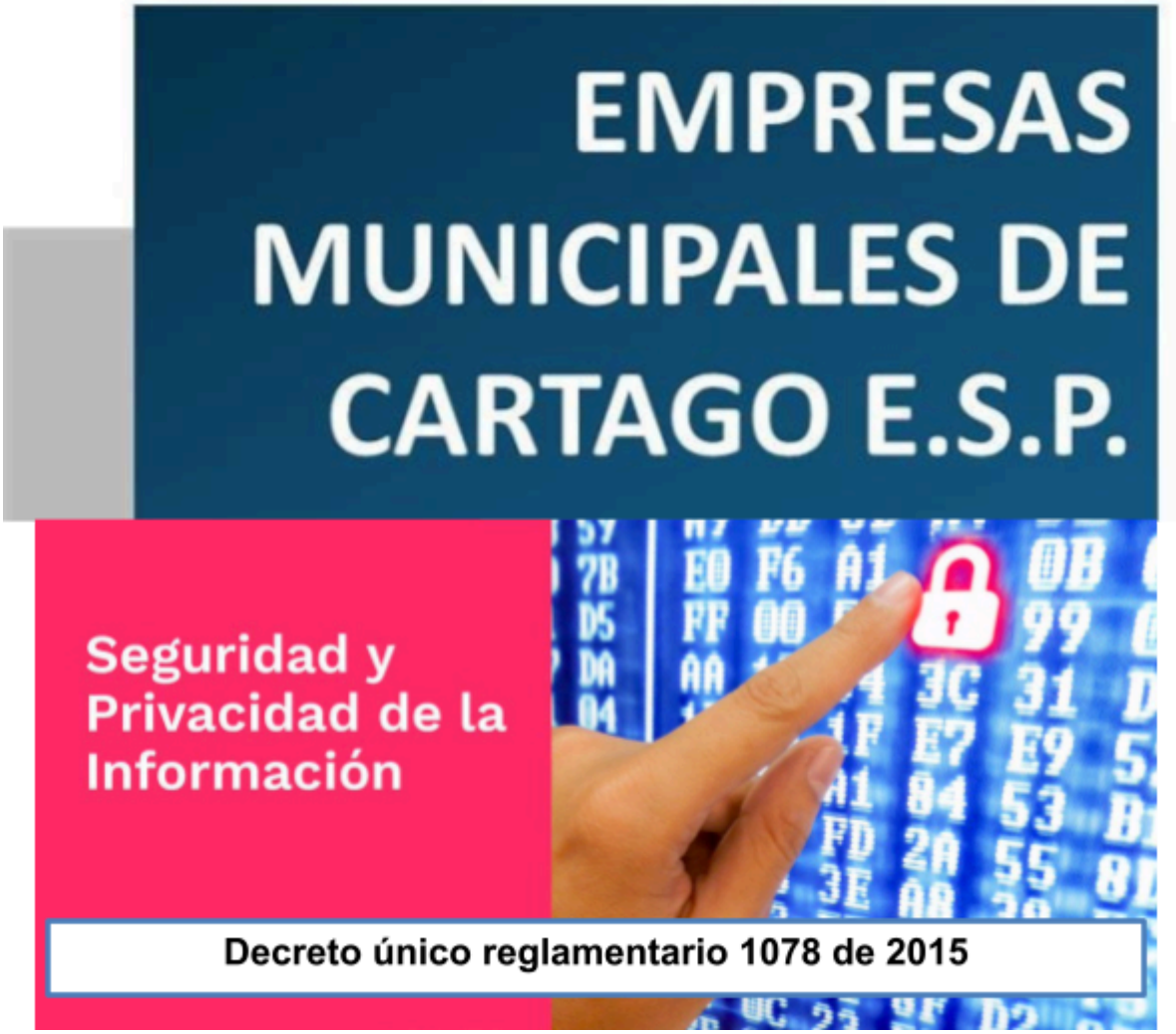
EMPRESAS
MUNICIPALES DE
CARTAGO E.S.P.
Seguridad y
Privacidad de la
Información
Decreto único reglamentario 1078 de 2015

CONTENIDO

INTRODUCCIÓN

Las Empresas Municipales de Cartago E.S.P.,en adelante EMCARTAGO E.S.P., es una Sociedad por Acciones, de carácter oficial, organizada en forma de Empresa de Servicios Públicos Domiciliarios(E.S.P.),cuyo objeto social corresponde entre otros a la prestación del servicio público domiciliario de acueducto, alcantarillado y de sus usuarios. EMCARTAGO E.S.P. en el presente documento adopta el Modelo de Seguridad y Privacidad de la Información y las comunicaciones a través de la estrategia de Gobierno en línea haciendo referencia a las políticas y definiciones o contenido relacionado, publicado en el compendio de las normas técnicas colombianas NTC ISO/IEC 27000 vigentes, así como a los anexos con derechos reservados por parte de ISO/ICONTEC.

1. GENERALIDADES DEL MANUAL

1.1 OBJETIVO

Establecerlas políticas y procedimientos para las buenas prácticas en Seguridad y Privacidad de la información que es responsabilidad de EMCARTAGO E.S.P para contribuir con el incremento de la transparencia en gestión y los lineamientos para las mejores prácticas en seguridad.

1.2 ALCANCE

La Política de Seguridad y Privacidad de la Información es aplicable a todos los procesos base de que son responsabilidad de EMCARTAGO E.S.P, su sistemas de información, herramientas de soportes y equipos de infraestructura y los empleados en el tratamiento de la información.

1.3 JUSTIFICACIÓN

El Modelo de Seguridad y Privacidad de la Información, para dar cumplimiento a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de gobierno en línea. Mediante el aprovechamiento de las TIC y el modelo de seguridad y privacidad de la información, EMCARTAGO E.S.P. trabaja en el fortalecimiento de la seguridad de la información en las entidades, con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, todo esto acorde con lo expresado en la legislación Colombiana.

1.4 DEFINICIONES

- **Activo:** en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.
- **Amenaza:** causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.
- **Amenaza informática:** la aparición de una situación potencial o actual donde una persona tiene la capacidad de generar una agresión cibernética contra la población, el territorio, la organización política del Estado (Ministerio de Defensa de Colombia).
- **Análisis de riesgos:** proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.
- **Anonimización del dato:** eliminar o sustituir algunos nombres de personas (físicas o jurídicas); direcciones y demás información de contacto, como números identificativos, apodos o cargo.
- **Autenticidad:** propiedad de que una entidad es lo que afirma ser. (ISO 27000.es, 2012).
- **Ciberseguridad:** capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.
- **Ciberespacio:** ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701).
- **Confidencialidad:** propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Control:** comprenden las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.
- **Custodio de activo de información:** identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la Veeduría Distrital, que tiene la responsabilidad de administrar y hacer efectivo los controles que el propietario del activo haya definido, con base en los controles de seguridad disponibles en la entidad.

- **Datos abiertos:** son datos primarios o sin procesar puestos a disposición de cualquier ciudadano, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.
- **Datos biométricos:** parámetros físicos únicos de cada persona que comprueban su identidad y se evidencian cuando la persona o una parte de ella interacciona con el sistema (huella digital o voz).
- **Datos personales sensibles:** se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.
- **Dato privado**: es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.
- **Dato público:** es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en

documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

- **Dato semiprivado:** es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.
- **Disco duro**: disco de metal cubierto con una superficie de grabación ferro magnético. Haciendo una analogía con los discos musicales, los lados planos de la placa son la superficie de grabación, el brazo acústico es el brazo de acceso y la púa (aguja) es la cabeza lectora/grabadora. Los discos magnéticos pueden ser grabados, borrados y regrabados como una cinta de audio.
- **Disponibilidad:** propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- **DVD:** Disco Versátil (video) Digital. En la actualidad constituye el natural sucesor del CD para la reproducción de sonido e imagen de calidad.
- **Evento de seguridad de la información:** ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.
- **Gestión de claves:** son controles que realizan mediante la gestión de claves criptográficas.
- **Gestión de incidentes de seguridad de la información:** procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
- **Gestión de riesgos:** actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.
- **Habeas data:** derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.
- **Impacto:** el coste para la empresa de un incidente -de la escala que sea- , que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.
- **Incidente de seguridad de la información:** evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Información:** La información está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.
- **Integridad:** la propiedad de salvaguardar la exactitud y complejidad de la información.
- **Inventario de activos:** lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. (ISO 27000.es, 2012)
- **No repudio**: servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido). (ISO-7498-2).

- **Parte interesada (*Stakeholder*):** persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
  Plan de continuidad del negocio: plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.
- **Plan de tratamiento de riesgos**: documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
- **Proceso**: conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas. (ISO 27000.es, 2012)
- **Propietario de activo de información:** identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.
- **Riesgo:** posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones. (ISO Guía 73:2002).
- **Responsable del tratamiento:** persona natural o jurídica, pública o privada. Que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.
- **Segregación de tareas:** reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.
- **Seguridad de la información:** preservación de la confidencialidad, integridad y disponibilidad de la información.
  Sistema de Gestión de Seguridad de la Información (SGSI): conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.
- **Titular de la información:** es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley.
- **Trazabilidad:** cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociada de modo inequívoco a un individuo o entidad.
- **Vulnerabilidad:** debilidad de un activo o control que pueda ser explotado por una o más amenazas. (ISO 27000.es, 2012).

1.5. PRINCIPIOS

Principio	Definición
Legalidad	El Tratamiento de los datos personales, se sujeta a las normas expedidas y vigentes sobre la materia.
Finalidad	El Tratamiento de los datos personales recolectados, almacenados Y manejados por el responsable obedece a una finalidad legítima de acuerdo con la Constitución y la Ley y está informada al Titular mediante los mecanismos autorizados para ello.
Libertad	Los datos personales no podrán ser obtenidos o divulgados sin previa autorización y cuentan con autorización del Titular acorde con los mecanismos indicados por las normas vigentes o en ausencia demanda legal o judicial que releve el consentimiento.
Veracidad o calidad	La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
Transparencia	En el Tratamiento de los datos se garantiza el derecho del Titular a obtener del responsable del Tratamiento o del encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.
Acceso y circulación restringida	El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la Ley.
Seguridad	La información sujeta a Tratamiento por parte del responsable tiene las medidas técnicas, humanas y administrativas aceptadas, necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
Confidencialidad	Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento.

1.6. VIGENCIA MANUAL

La documentación presentada como Política General de Seguridad de la Información entrará en vigor desde el momento en que sea aprobado por la Gerencia. Este documento deberá ser constantemente revisado y actualizado de acuerdo con las exigencias de la organización o en el momento de haber algún cambio notorio en la infraestructura tecnológica.

Es responsabilidad de la Gerencia acordar los tiempos para la implementación de cada una de las políticas, mediante instructivos desarrollados juntamente con la Oficina de Informática.

2. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2.1. INFORMACIÓN DELRESPONSABLEDELTRATAMIENTODEDATOS

Razón Social	Empresas Municipales de Cartago ESP
Nit	836000349-8
Ciudad	Cartago
Dirección	Cl 135A-35
Teléfono	(572)2110060
Matricula Mercantil	29356
Naturaleza	Publica
Cogido CIIU	3514Comercializaciónde Energía Eléctrica

2.2. OFICIAL DE PRIVACIDAD

1 DOCUMENTOS DE REFERENCIA

- Manual de Gobierno Digital
- Gobierno TIC
- Ley 1273 de 2009 del Congreso de la República. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1581 de 2012 del Congreso de la República. Por el cual se dictan disposiciones generales para la protección de datos personales. HABEAS DATA.
- Ley 1712 de 2014 del Congreso de la República. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Decreto 2609 de 2012 de la Presidencia de la República. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- Decreto 1377 de 2013 de la Presidencia de la República. Por el cual se reglamenta parcialmente la Ley 1581 de 2012 sobre la protección de datos personales.
- Decreto 2573 de 2014 de la Presidencia de la República. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
- Decreto 103 de 2015 de la Presidencia de la República. Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto Único Reglamentario 1078 de 2015, Título 9 capítulo 1, Estrategia del Gobierno en Línea. Sección 2, Artículo 2.2.9.1.2.1 numeral 4 define el componente de Seguridad y Privacidad de la Información.
- Decreto 415 de 2016 de la Presidencia de la República. Lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
- Norma Técnica ISO/IEC 27001 de 2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos.

2 DESARROLLO DEL DOCUMENTO

DESCRIPCIÓN GENERAL DE POLITICAS

3 ANEXOS

10. CONTROL DE ELABORACIÓN

Elabora:	Revisa:	Aprueba:
_____ Carlos Alberto Abad Moreno	_____	_____
Fecha:	Fecha	Fecha

11. CONTROL DE CAMBIOS

RELACION DE CAMBIOS EN EL DOCUMENTO		
VERSIÓN	**FECHA**	**CAMBIO REALIZADO**
V1		Creación