ALCALDÍA DE
CANDELARIA
VALLE DEL CAUCA - COLOMBIA - SURAMÉRICA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Vigencia 2021

Calle 9 No. 7 - 69
Código Postal: 763570
Teléfono: (57 2) 264 6209 / 2646344
www.candelaria-valle.gov.co
contacto@candelaria-valle.gov.co
Candelaria - Valle
Colombia - Enero 31 de 2020 ©

CON EXPERIENCIA AVANZAMOS

TABLA DE CONTENIDO

1. INTRODUCCIÓN

EL Municipio de Candelaria de Candelaria ha venido implementando la Estrategia de Gobierno en línea hoy llamada Gobierno Digital.

La Política de Gobierno Digital establecida mediante el Decreto 1008 de 2018 cuyas disposiciones se compilan en el decreto 1078 de 2015, "Decreto único reglamentario del sector TIC" específicamente en el Capítulo 1 titulo 9, parte 2, libro 2, forma parte del Modelo Integrado de Planeación y Gestión (MIPG) y se integra con las políticas de Gestión y Desempeño Institucional en la dimensión operativa de Gestión para Resultados con Valores, que busca promover una adecuada gestión interna en las entidades y un buena relación con el ciudadano, a través de la participación y la prestación de servicios de calidad.

Candelaria Adopto el Modelo mediante el Decreto Nro. 162 de 2019

El Modelo Integrado de Planeación y Gestión. Dimensión 3 Gestión con valores para resultados con la Política Nro. 11 GOBIERNO DIGITAL. Cuyo objetivo es el uso y el aprovechamiento de las TIC consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital y que tiene dos componentes fundamentales TIC PARA EL ESTADO, TIC PARA LA SOCIEDAD con tres habilitadores transversales Seguridad de la Información Arquitectura y servicios ciudadanos digitales y con ellos cinco propósitos Servicios Digitales de Confianza y Calidad, Procesos Internos Seguros y Eficientes, Decisiones basadas en Datos, Empoderamiento ciudadano a través de un Estado Abierto y territorio y ciudades inteligentes a través de las tic.

Política Nro. 12 SEGURIDAD DIGITAL la implementación de la política se hará a través de la adopción e implementación del Modelo de Gestión de Riesgo de Seguridad Digital

El Municipio de Candelaria Valle Cuenta con un comité de Seguridad de la Información que fue creado mediante el Decreto No 185 de junio 25 de 2008 de igual manera tiene la Política de Seguridad de la Información Actualizada en Julio de 2017.

Teniendo en cuenta lo anterior, se actualiza el presente documento dando cumplimiento a lo establecido en el Decreto 612 de 2018, actualizando el Plan de seguridad de Implementación de Seguridad y privacidad de la Información al interior del Municipio de Candelaria valle

2. OBJETIVO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Establecer las Actividades que están contempladas en el modelo de Seguridad y Privacidad de la Información y en la Política de Seguridad de la información del Municipio de Candelaria alineados con la NTC/IEC ISO 27001:2013.

3. POLITICA DE SEGURIDAD DE LA INFORMACION

El municipio de Candelaria cuenta con la política de seguridad de la información que fue propuesta por el comité de Seguridad de la Información (CSI) para la alcaldía y se encuentra basadas en la Norma NTC/ISO IEC 17799 con su equivalente NTC/ISO/ IEC 27001,27002 como un marco de referencia para la gestión de la seguridad de la información en l Administración Municipal de Candelaria.

La Norma ISO/IEC 27001 avala la adecuada implantación, gestión y operación de todo lo relacionado con un SGSI, siendo la norma más completa que existe en la implantación de controles, métricas e indicadores que permiten establecer un marco adecuado de gestión de la seguridad de la información para las organizaciones.

Esta norma ha sido elaborada para brindar un modelo para el establecimiento, implementación y operación, seguimiento, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI). Esta norma adopta el modelo de procesos “Planificar, Hacer, Verificar, Actuar (PHVA) que aplica para estructurar todos los procesos del SGSI.

3.1. OBJETIVO DE LA POLITICA DE SEGURIDAD DE LA INFORMACION

Esta Política tiene como objetivo proteger los recursos de información de la Alcaldía y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurar la implementación de las medidas de seguridad comprendidas en esta política, identificando los recursos y partidas presupuestales correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.

4. ALCANCE

La Política de Seguridad de la Información se dicta en cumplimiento de la disposición legal vigente, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la

Administración Central del municipio de Candelaria, que adelante se denomina Alcaldía.

Esta Política se aplica a todo el ámbito de la Alcaldía, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros. Debe ser conocida y cumplida por toda la planta de personal de la Alcaldía, tanto se trate de servidores públicos, contratistas, personal temporal y otras personas relacionadas con terceras partes que utilicen recursos informáticos de la Administración Central del municipio de candelaria

5. TERMINOS Y DEFINICIONES

- Administración de Riesgos. Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podría afectar a la información.

- Auditabilidad. Define que todos los eventos de un sistema deben poder ser registrados para su control posterior

- Autenticidad. Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

- Confiabilidad de la Información. Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de la misiones y funciones.

- Confidencialidad. Se garantiza que la información se accesible solo a aquellas personas autorizadas a tener accesos a la misma.

- Disponibilidad. Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que requieran.

- Evaluación de Riesgos. Se entiende a la amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma. La probabilidad de que ocurran y su potencial impacto en la operatoria de la Alcaldía.

- Información. Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, graficas cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en pape, en pantallas de computadoras, audiovisual u otro.

- Incidente de Seguridad. Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, la integridad o disponibilidad, la legalidad y confiabilidad de la información. Pude ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenazas de romper los mecanismos de seguridad existentes.

- Integridad. Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

- Legalidad. Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a la que está sujeta la Alcaldía.

- No repudio. Se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

- Protección a la Duplicación. Consiste en asegurar que una transacción solo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

- Sistema de Información- se refiere al Hardware y Software operado por la Alcaldía o por terceros que procese información en su nombre, para llevar a cabo una función propia de la Alcaldía, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

6. MARCO NORMATIVO

ID	NORMA	AÑO	DESCRIPCIÓN
N001	Ley 527	1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones
N002	Decreto 1122	1999	Por el cual se dictan normas para suprimir trámites, facilitar la actividad de los ciudadanos, contribuir a la eficiencia y eficacia de la Administración Pública y fortalecer el principio de la buena fe.
N003	Decreto 1151	2008	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones

N004	Ley 1341	2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
N005	Ley 1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
N006	Decreto 2693	2012	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.
N007	Ley 1712	2014	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.
N008	Decreto 2573	2014	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.
N009	Decreto 0103	2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
N010	Decreto 1078	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de tecnología de la Información y las Comunicaciones.
N011	Decreto 415	2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
N012	NTC-ISO/IEC 27001	2013	Tecnología de la información, técnicas de seguridad. Sistema de gestión de Seguridad de la información
N013	NTC-ISO/IEC-27002		Tecnología de la información, técnicas de seguridad. Código de practica para la gestión de seguridad de la información
N014	NTC-ISO/IEC-27005		Tecnología de la información, técnicas de seguridad. Gestión del riesgo en la seguridad de la información
N015	Ley 1273 de 2009	2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado “de la protección de la información y los datos” y se preservan integralmente los sistemas que utilicen las

			tecnologías de la información y las comunicaciones, entre otras disposiciones
N016	Ley 594 de 2000		Ley General de Archivos
N017	Decreto 2609	2012	Por medio del cual se reglamenta el Titulo 5 de la ley General de Archivo del año 2000. Incluye aspectos que se debe considerar para la adecuada gestión de los documentos electrónicos

7. COMITÉ DE SEGURIDAD DE LA INFORMACION

El Comité de Seguridad de la información, es un equipo de trabajo interdisciplinario que desarrolla labores de asesoría, definición de estándares, de coordinación, de control, en la formulación de políticas en materia de seguridad de la información. Creado mediante el decreto 185 del 25 de junio de 2008 e integrado por:

- El Alcalde o su delegado (a)
- El Servidor público con Funciones de Control Interno Municipal
- El Director del Departamento Administrativo de Planeación e informática
- El Secretario de hacienda Municipal
- Servidor Público responsable del área de Informática de la Alcaldía
- El Secretario de Desarrollo Administrativo Municipal
- Un asesor externo de seguridad (si existiera)

7.1. Responsable de la seguridad Informática. Es el Servidor público que cumple las funciones de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes de la Alcaldía que así lo requieran. Esta labor está a cargo del profesional universitario responsable del Área de informática de la Alcaldía. Todos los Secretarios y Directores titulares de Dependencias son responsables de la implementación de esta política de seguridad de la información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo. La política de Seguridad de la información es de aplicación obligatoria para todo el personal de la Alcaldía, cual quera que sea su vinculación, el área de trabajo y el nivel de las tareas que desempeñe.

7.2. Comité de Seguridad de la información. Procederá a revisar y proponer al Consejo de Gobierno para su aprobación la política de Seguridad de la Información y las funciones generales en materia de seguridad de la información; monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes; tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.

8. PLAN DE IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD DE A INFORMACIÓN

GESTION	ACTIVIDADES	TAREAS	RESPONSABLES DE LAS TAREAS	FECHA DE PROGRAMACION	
				FECHA INICIO	FECHA FIN
ACTIVOS DE INFORMACION	Definir los lienamientos para el levantamiento de los activos de informacion	Actualización de Metodologias e Instrumento de levantamiento de activos de informacion	Equipo Activo de Informacion	FEBRERO AÑO 2021	FEBRERO AÑO 2021
	Levantamiento Activo de Informacion	Socializacion guia de Activos de Informacion	Equipo Activo de Informacion	FEBRERO AÑO 2021	JUNIO AÑO 2021
		Validar activos de Informacion en el instrumento levantado en la vigencia Anterior	Enlace de Cada proceso Equipo de Activos de Informacion	JUNIO AÑO 2021	JUNIO AÑO 2021
		Identificar nuevos Activos de Información en cada dependencia y /o secretaria	Enlace de Cada proceso Equipo de Activos de Informacion	JUNIO AÑO 2021	JUNIO AÑO 2021
		Revisar los Instrumentos de Activos de Informacion y realimentar a las Areas con las modificaciones	Equipo Activo de Informacion	JULIO AÑO 2021	JULIO AÑO 2021
		Realizar correcciones a los instrumentos de activos de informacion, cambios fisicos de la ubicación de activos de informacion	Enlace de Cada proceso	JULIO AÑO 2021	JULIO AÑO 2021
		Realizar informe de Actualizacion a los Activos de Informacion por alguna novedad que se presente como alguna actualizacion a los procesos al que pertenezca el activo, pr adicion de actividades al proceso, po cambio o migraciones de sistemas de informacion, materializacion de los riegos que cambie la criticidad del activo	Enlace de Cada proceso	JULIO AÑO 2021	DICIEMBRE AÑO 2021
	Publicacion de Activos de Informacion	Validar y aceptar los activos informacion para su publicacion en la pagina web del Municipio de Candelaria	Enlace de Cada proceso Equipo de Activos de Informacion	AGOSTO AÑO 2021	AGOSTO AÑO 2021
		Consolidar el instrumento de Activo de informacion	Equipo Activo de Informacion	AGOSTO AÑO 2021	AGOSTO AÑO 2021
		Publicar el instrumento de actvos de informacion consolidados en la pagina web del municipio	OFICINA TIC (INFORMATICA Y COMUNICACIONES)	AGOSTO AÑO 2021	AGOSTO AÑO 2021
	Registro Activos de Informacion ley 112	Actulizacion de los registros de Activos de Informacion con el insumo de los instrumentos de activos de informacion	Equipo Activo de Informacion	SEPTIEMBRE AÑO 2021	SEPTIEMBRE AÑO 2021
		Enviar Control de legalidad el instrumento de registro de activos de informacion	Equipo de Activo de Informacion con Asesoria Juridica	SEPTIEMBRE AÑO 2021	SEPTIEMBRE AÑO 2021
		Publicacion del registro Activos de informacion en la pagina web Municipio de Candelaria	OFICINA TIC (INFORMATICA Y COMUNICACIONES)	SEPTIEMBRE AÑO 2021	SEPTIEMBRE AÑO 2021
	Reporte de Datos Personales	Reportar al oficial de datos Personales o Seguridad de la informacion, la informacion recolectada en el isntrucmento de activos de informacion, correspondiente a base de datos	Equipo Activo de Informacion	SEPTIEMBRE AÑO 2021	SEPTIEMBRE AÑO 2021

GESTION	ACTIVIDADES	TAREAS	RESPONSABLES DE LAS TAREAS	FECHA DE PROGRAMACION	
				FECHA INICIO	FECHA FIN
GESTION DE RIESGOS	Actualizacion de liniamientos de Riesgos	Actulizar la Politica y metodologias de Gestion de Riesgos	Equipo de Gestion de Riesgos	MARZO AÑO 2021	MARZO AÑO 2021
	Sensiblizacion	Socializacion Guia de Herramientas Gestion de Riesgos de Seguridad y Privacidad de la Informacion, seguridad digital y continuidad de operaciones	Equipo de Gestion de Riesgos	ABRIL AÑO 2021	ABRIL AÑO 2021
	Idenfcacion de Riesgos Seguridad y privacidad de la informacion, seguridad Digital y continuidad de operaciones	Identificacion, Analisis y Evaluacion de Riesgos de Seguridad y Privacidad de la informacion, Seguridad Digital y continuidad de operación	Equipo de Gestion de Riesgos	ABRIL AÑO 2021	ABRIL AÑO 2021
		Realimetar , revision y verificacion de los Riesgos Identificados	Equipo de Gestion de Riesgos	ABRIL AÑO 2021	ABRIL AÑO 2021
	Aceptacion de Riesgos Identificados	Aceptacion, Aprobacion Riesgos identifiacdos y Planes de Tratamiento	Equipo de Gestion de Riesgos	JUNIO AÑO 2021	NOVIEMBRE AÑO 2021
	Publicacion de los Riesgos	Publicacion de la Matriz de Riesgos en el Sistema de Informacion Intrafile	Equipo de Gestion de Riesgos	JUNIO AÑO 2021	NOVIEMBRE AÑO 2021
	Seguimiento Fase de Tratamiento	Seguimiento Estado de Planes de Tramientos de riesgos identificados y verificados de evidencias	Equipo de Gestion de Riesgos	JUNIO AÑO 2021	DICIEMBRE AÑO 2021
	Evaluacion del Riesgo residuales	Evaluación de Riesgos residuales	Equipo de Gestion de Riesgos	JUNIO AÑO 2021	DICIEMBRE AÑO 2021
	Mejoramiento	Identificacion de Oportunidades de mejora acorde a los resultados obtenidos durante la evaluacion de riesgos residuales	Equipo de Gestion de Riesgos	JUNIO AÑO 2021	DICIEMBRE AÑO 2021
		Actulizacion de Guias Gestion de Riesgos de seguridad de la informacion de acuerdo a los cambios solicitados	Equipo de Gestion de Riesgos	JUNIO AÑO 2021	DICIEMBRE AÑO 2021
	Monitoreo	Generacion Presentacion y reporte de indicadores	Equipo de Gestion de Riesgos	JUNIO AÑO 2021	DICIEMBRE AÑO 2021