

	SISTEMA INTEGRADO DE GESTIÓN DE LA CALIDAD - SGC Y MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG	CÓDIGO	PO-SD-01
		VERSIÓN	1.0
		FECHA	01/02/2022
	POLÍTICA DE SEGURIDAD DIGITAL ALCALDÍA LOCAL ISLA DEL CASCAJAL	PAGINA	1 DE 9

CONTENIDO

	Pag.
INTRODUCCIÓN	
1. OBJETIVOS	03
2. ALCANCE	03
3. MARCO LEGAL	03
4. TERMINOS Y DEFINICIONES	03
5. POLITICA DE SEGURIDAD DIGITAL	06
5.1. NIVEL DE CUMPLIMIENTO	06
5.2. IMPLEMENTACION DE ESTRATEGIAS	06
6. COMUNICACIÓN	07
7. VIGENCIA DE LA POLÍTICA DE SEGURIDAD DIGITAL	07
8. EVALUACION Y SEGUIMIENTO	09
9. MODIFICACION A DE LA POLÍTICA DE SEGURIDAD DIGITAL	09
10. RUTA DE LA POLÍTICA	09

	SISTEMA INTEGRADO DE GESTIÓN DE LA CALIDAD - SGC Y MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG	CÓDIGO	PO-SD-01
		VERSIÓN	1.0
		FECHA	01/02/2022
	POLÍTICA DE SEGURIDAD DIGITAL ALCALDÍA LOCAL ISLA DEL CASCAJAL	PAGINA	2 DE 9

INTRODUCCIÓN

El Modelo Integrado de Planeación y Gestión MIPG es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio, según dispone el Decreto1499 de 2017.

Mejorar la capacidad del Estado para cumplirle a la ciudadanía, incrementando la confianza de la ciudadanía en sus entidades y en los servidores públicos, logrando mejores niveles de gobernabilidad y legitimidad del aparato público y generando resultados con valores a partir de una mejor coordinación interinstitucional, compromiso del servidor público, mayor presencia en el territorio y mejor aprovechamiento y difusión de información confiable y oportuna es una de los objetivos de la puesta en marcha del Modelo Integrado de Planeación y Gestión MIPG.

Se hace necesaria que la Alcaldía Local Isla del Cascajal formule e implemente la Política de Seguridad Digital para establecer lineamientos y estrategias para que los recursos TIC obedezcan a las directrices de seguridad y evitar que se creen vulnerabilidades que impacten la Entidad.

Actualmente, el creciente uso del entorno digital en Colombia para desarrollar actividades económicas y sociales, acarrea incertidumbres y riesgos inherentes de seguridad digital que deben ser gestionados permanentemente. No hacerlo, puede resultar en la materialización de amenazas o ataques cibernéticos, generando efectos no deseados de tipo económico o social para el país, y afectando la integridad de los ciudadanos en este entorno.

Por lo anterior, la Política de Seguridad Digital de la Alcaldía Local Isla del Cascajal pretende proporcionar una serie de reglas, lineamientos y mecanismos para garantizar disponibilidad, confidencialidad e integridad los activos informáticos conectados o no a la red interna y a la información que ellos procesan o intercambien.

	SISTEMA INTEGRADO DE GESTIÓN DE LA CALIDAD - SGC Y MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG	CÓDIGO	PO-SD-01
		VERSIÓN	1.0
		FECHA	01/02/2022
	POLÍTICA DE SEGURIDAD DIGITAL ALCALDÍA LOCAL ISLA DEL CASCAJAL	PAGINA	3 DE 9

1. OBJETIVOS

El objetivo de la política es contrarrestar el incremento de las amenazas informáticas que pueden afectar significativamente la institución y el correcto desarrollo normativo y legal de las mismas fortaleciendo la institucionalidad de la entidad

2. ALCANCE

La Política de Seguridad Digital pretende identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades.

Esta política aplica para todos los procesos institucionales, pues la eficiencia de todos y cada uno de los procesos afecta directa o indirectamente los recursos institucionales, por lo tanto, será aplicable a todos los empleados, contratistas, proveedores, visitantes y ciudadanos de la Alcaldía y de acuerdo al nivel jerárquico se aplicaran las restricciones del caso.

3. MARCO LEGAL

Decreto 1499 de 2017: Por medio del cual se implementa el Modelo Integrado de Planeación y Gestión – MIPG.

Decreto 2609 de 2012: Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.

Decreto 2693 de 2012: Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

Ley 599 DE 2000: Por la cual se expide el Código Penal. Se crea el bien jurídico de los derechos de autor e incorpora algunas conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y manifiesta que el acceso abusivo a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa.

Ley 1273 DE 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.

	SISTEMA INTEGRADO DE GESTIÓN DE LA CALIDAD - SGC Y MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG	CÓDIGO	PO-SD-01
		VERSIÓN	1.0
		FECHA	01/02/2022
	POLÍTICA DE SEGURIDAD DIGITAL ALCALDÍA LOCAL ISLA DEL CASCAJAL	PAGINA	4 DE 9

Ley 1341 DE 2009: Por medio de la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y comunicaciones - TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

NTC 27001:2006: Sistema de Gestión de Seguridad de la Información (SGSI).

ISO 27002:2005: Esta norma proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar e implantar o mantener sistemas de gestión de la seguridad de la información.

ISO/IEC 27001:2005: Es la evolución certificable del código de buenas prácticas ISO 17799. Define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información.

4. TÉRMINOS Y DEFINICIONES

Activo de Información: Es todo aquello que en la entidad es considerado importante o de alta validez para la misma ya que puede contener información importante como son en las Bases de Datos con usuarios, contraseñas, números de cuentas, etc.

Amenaza: Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.

Análisis de riesgos: Uso sistemático de la información para identificar las fuentes y estimar el riesgo NTC-ISO /IEC 27001.

Confidencialidad: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Copias de respaldo: Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Firewall: Un firewall es un dispositivo de seguridad diseñada para permitir, monitorear, restringir o limitar las conexiones en determinados puertos de comunicación de la red interna o externa, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.

Hardware: Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

Incidentes de seguridad de la información: Se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información.

Información: Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

	SISTEMA INTEGRADO DE GESTIÓN DE LA CALIDAD - SGC Y MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG	CÓDIGO	PO-SD-01
		VERSIÓN	1.0
		FECHA	01/02/2022
	POLÍTICA DE SEGURIDAD DIGITAL ALCALDÍA LOCAL ISLA DEL CASCAJAL	PAGINA	5 DE 9

Infraestructura tecnológica: Es el conjunto de hardware y software para el funcionamiento de los diferentes servicios con los que cuenta la entidad.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

MSPI: Modelo de Seguridad y Privacidad de la Información.

No Repudio: Proporciona la prueba ante una tercera parte de que tanto una entidad como una persona han participado en una comunicación.

Política de Seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:20005): intención y dirección general expresada formalmente por la Dirección.

Riesgo: Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.

Riesgo de Gestión: posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

Riesgo de Seguridad Digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgo Inherente: Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

Riesgo residual: Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.

Gestión de Riesgo: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Seguridad de la Información: es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

Seguridad perimetral: corresponde a la integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos y lógicos, detección de tentativas de intrusión y/o disuasión de intrusos en instalaciones especialmente sensibles.

Servidor: Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia

	SISTEMA INTEGRADO DE GESTIÓN DE LA CALIDAD - SGC Y MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG	CÓDIGO	PO-SD-01
		VERSIÓN	1.0
		FECHA	01/02/2022
	POLÍTICA DE SEGURIDAD DIGITAL ALCALDÍA LOCAL ISLA DEL CASCAJAL	PAGINA	6 DE 9

SGSI: Sistema de Gestión de Seguridad de la información. Vulnerabilidad: Es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

VPN: Virtual Private Network, una red privada virtual que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como internet.

5. POLÍTICA DE SEGURIDAD DIGITAL

La Alcaldía Local Isla del Cascajal, con el fin de abordar las incertidumbres, los riesgos, las amenazas, las vulnerabilidades y los incidentes digitales, adoptara la política de seguridad digital que en su conjunto tendrá como fin contrarrestar el incremento de las amenazas informáticas que pueden afectar significativamente la institución y el correcto desarrollo normativo y legal de las mismas fortaleciendo la institucionalidad de la entidad.

5.1. NIVEL DE CUMPLIMEINTO

Todas las personas cubiertas por el alcance y aplicabilidad se espera que se adhieran en un 100% a la política. Las políticas serán objeto de evaluación aplicando mecanismos de mejoramiento continuo que involucren participación, compromiso, cooperación, adaptación e inversión.

5.2. IMPLEMENTACIÓN DE ESTRATEGIAS

A continuación se describen las estrategias que se implementarán para alcanzar la política de seguridad digital.

- Implementar iniciativas apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias digitales para afrontar las amenazas y los riesgos que atentan contra la seguridad digital.
- Brindar capacitación especializada en seguridad de la información y seguridad digital.
- Definir, implementar, operar y mejorar de forma continua el Plan de Seguridad y privacidad de la información, soportado en lineamientos claros alineados a las necesidades, a la normatividad y a los requerimientos regulatorios.
- Definir responsabilidades frente a la seguridad de la información.
- Aplicar controles de acuerdo con la clasificación de la información salvaguardada y en custodia por cada uno de los funcionarios, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta.

	SISTEMA INTEGRADO DE GESTIÓN DE LA CALIDAD - SGC Y MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG	CÓDIGO	PO-SD-01
		VERSIÓN	1.0
		FECHA	01/02/2022
	POLÍTICA DE SEGURIDAD DIGITAL ALCALDÍA LOCAL ISLA DEL CASCAJAL	PAGINA	7 DE 9

- Realizar ejercicios de auditoria y monitoreo de la operación de sus procesos que involucren la plataforma tecnológica para minimizar los riesgos asociados al manejo de los recursos tecnológicos y las redes de datos.
- Implementar controles de acceso a la información, sistemas y recursos de red.
- Adoptar una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información e implementar estrategias de mejoramiento continuo
- Elaborar procedimientos de acuerdo a la normatividad que permitan minimizar los riesgos que puedan generar los eventos

6. COMUNICACIÓN.

La divulgación de la Política debe ser transmitida e implementada a través de las diferentes áreas o procesos que conforman la estructura organizacional y jerarquía de la administración Local.

7. VIGENCIA DE LA POLÍTICA DE SEGURIDAD DIGITAL

La política de seguridad digital rige a partir del momento en que sea aprobada por la Alta Dirección de la Alcaldía Local Isla del Cascajal.

8. EVALUACIÓN Y SEGUIMIENTO.

El seguimiento es un instrumento indispensable para la implementación adecuada de la política. Se trata de contar con la opción de supervisar el avance o, en su caso, los problemas que registre el desarrollo de la misma para de manera oportuna tomar acciones o medidas correctivas.

El seguimiento se realizara de manera mensual de acuerdo al Plan de Acción arrojado en el proceso de autodiagnóstico, y teniendo en cuenta las recomendaciones emitidas en los resultados FURAG en cuanto a la implementación de la Política de Seguridad Digital.

ESTRATEGIAS	UNIDAD DE MEDIDA	INDICADOR	RESPONSABLE	PROGRAMACION
Implementar iniciativas apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias digitales para afrontar las amenazas y los riesgos que atentan contra la seguridad digital	Estrategias para minimizar riesgos	Estrategias para minimizar riesgos implementada	Líderes de procesos	Entre enero hasta diciembre del año.

	SISTEMA INTEGRADO DE GESTIÓN DE LA CALIDAD - SGC Y MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG	CÓDIGO	PO-SD-01
		VERSIÓN	1.0
		FECHA	01/02/2022
	POLÍTICA DE SEGURIDAD DIGITAL ALCALDÍA LOCAL ISLA DEL CASCAJAL	PAGINA	8 DE 9

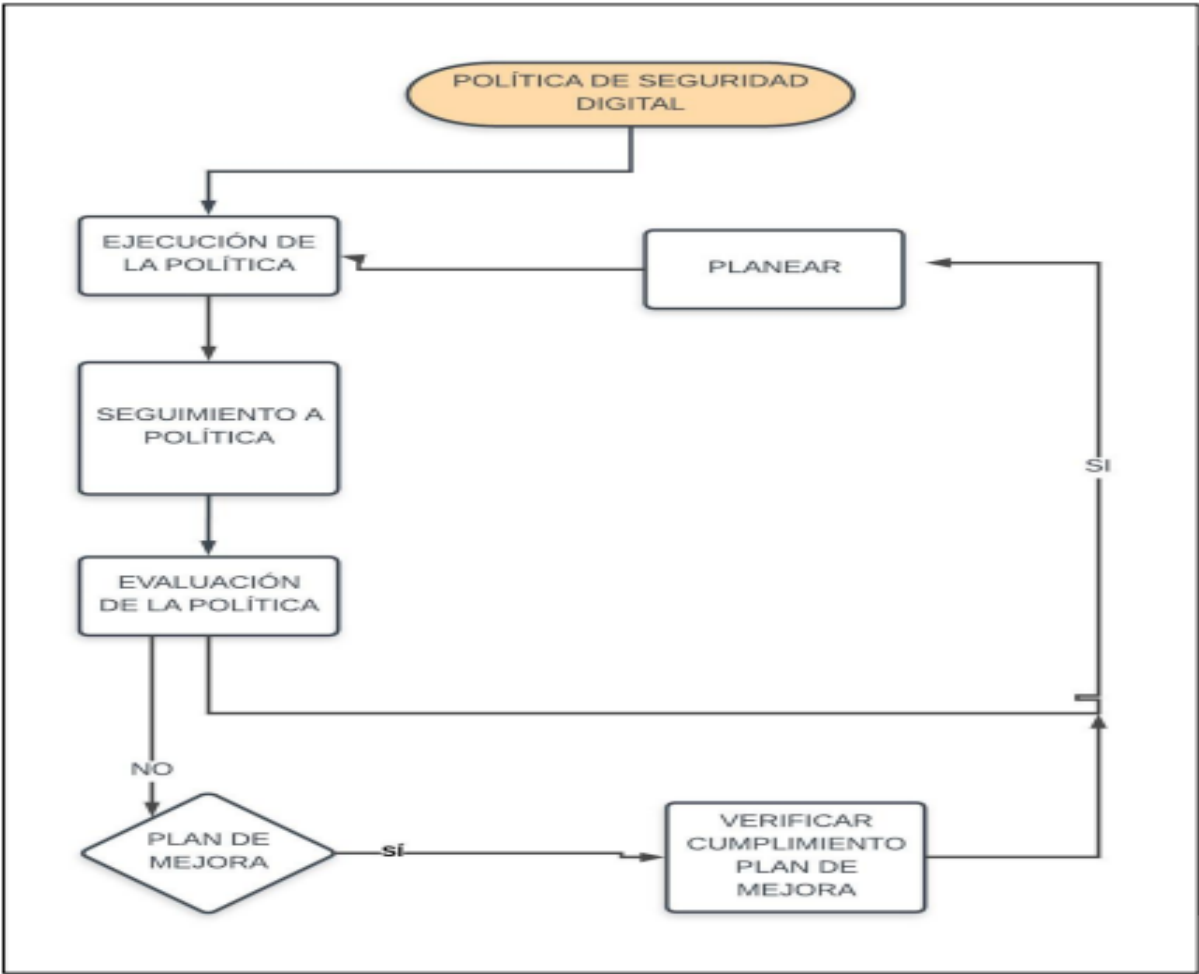
ESTRATEGIAS	UNIDAD DE MEDIDA	INDICADOR	RESPONSABLE	PROGRAMACIÓN
Brindar capacitación especializada en seguridad de la información y seguridad digital	Capacitación en seguridad de la información	Capacitación en seguridad de la información realizada	Líderes de procesos	Entre enero hasta diciembre del año.
Definir, implementar, operar y mejorar de forma continua el Plan de Seguridad y privacidad de la información, soportado en lineamientos claros alineados a las necesidades, a la normatividad y a los requerimientos regulatorios	Plan de Seguridad y privacidad de la Información	Plan de Seguridad y privacidad de la Información formulado e implementado	Líderes de procesos	Entre enero hasta diciembre del año.
Definir responsabilidades frente a la seguridad de la información.	Responsabilidades definidas	Responsabilidades definidas frente a seguridad de la información	Líderes de procesos	Entre enero hasta diciembre del año.
Aplicar controles de acuerdo con la clasificación de la información salvaguardada y en custodia por cada uno de los funcionarios, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta	Controles aplicados	Controles aplicados	Líderes de procesos	Entre enero hasta diciembre del año.
Realizar ejercicios de auditoria y monitoreo de la operación de sus procesos que involucren la plataforma tecnológica para minimizar los riesgos asociados al manejo de los recursos tecnológicos y las redes de datos	Auditoria y monitoreos realizados	Auditoria y monitoreos realizados	Líderes de procesos	Entre enero hasta diciembre del año.
Implementar controles de acceso a la información, sistemas y recursos de red	Controles realizados	Controles realizados	Líderes de procesos	Entre enero hasta diciembre del año.
Adoptar una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información e implementar estrategias de mejoramiento continuo	Estrategias de mejoramiento continuo	Estrategias de mejoramiento continuo implementadas	Líderes de procesos	Entre enero hasta diciembre del año.
Elaborar procedimientos de acuerdo a la normatividad que permitan minimizar los riesgos que puedan generar los eventos	Procedimientos	Procedimientos elaborados	Líderes de procesos	Entre enero hasta diciembre del año.

	SISTEMA INTEGRADO DE GESTIÓN DE LA CALIDAD - SGC Y MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN - MIPG	CÓDIGO	PO-SD-01
		VERSIÓN	1.0
		FECHA	01/02/2022
	POLÍTICA DE SEGURIDAD DIGITAL ALCALDÍA LOCAL ISLA DEL CASCAJAL	PAGINA	9 DE 9

9. MODIFICACIÓN A LA POLÍTICA DE SEGURIDAD DIGITAL

La política de seguridad digital de la Alcaldía Local Isla del Cascajal deberá revisarse o actualizarse mínimo cada dos (2) años o cuando las normas así lo exijan. Cualquier cambio será publicado y anunciado. Además, se conservarán las versiones anteriores de la presente política.

10. RUTA DE LA POLITICA



Control de cambio

FECHA:	RAZÓN DEL CAMBIO:	NUEVA VERSIÓN:
01/02/2022	Creación del documento	1.0

	ELABORÓ:	REVISÓ Y APROBÓ
Nombre:	Aracelly Arboleda Urbano	Julio Cesar Biojó Estacio
Cargo:	Profesional Universitario	Alcalde Local
Firma:	Original firmado	Original firmado