PUERTO COLOMBIA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

ALCALDÍA MUNICIPAL DE PUERTO COLOMBIA

ESTRATEGIA DE GOBIERNO DIGITAL
2020

E-mail Comunicaciones@puertocolombia-atlantico.gov.co
sistemas@puertocolombia-atlantico.gov.co
Tel (+57) 5 3854473 (+57) 5 3099327
Dir. Cra 4 n 2-18 Cod. Postal 081001

INFORMACIÓN DEL DOCUMENTO

Título	Política de Seguridad de la Información
Archivo	Entregable 3
Versión	3.0
Autor	Milena Cortes Pérez
Estado	Revisión

HISTORIAL DE CAMBIOS

Versión	Fecha	Descripción	Autor
1.0	2015/10/25		Juan Manuel Meza Barraza
2.0	2018/11/15		Juan Manuel Meza Barraza
3.0	2020		Milena Cortes Pérez

FIRMAS Y APROBACIONES

Nombre Aprobador	Entidad/Rol	Firma	Fecha
Ing, Juan Manuel Meza Barraza	Coordinador TIC		
Milena Cortes Pérez	Coordinadora TIC		

DERECHOS DE AUTOR

AUDIENCIA

Entidades públicas del orden territorial municipal, así como proveedores de servicios de Gobierno Digital y terceros que deseen adoptar el Modelo de seguridad de la información en el marco de la estrategia gobierno en línea.

Dependencias, funcionarios, proveedores y contratistas del Municipio de Puerto Colombia.

INTRODUCCION

Teniendo en cuenta lo establecido en el plan vive digital, liderado por el ministerio de las tecnologías de la información y comunicación, cuanto a la infraestructura, los servicios, las aplicaciones y los usuarios en el marco de un ecosistema digital; las recomendaciones brindadas en el plan nacional de desarrollo 2010-2014 en cuanto a la necesidad de reconocer la seguridad informática como un factor primordial para la apropiación de las TIC; la constante evolución de los mercados; y la dinámica de las entidades, se plantea a través de las tecnologías de la información, el cual deberá ser respaldo por una gestión, unas políticas y unos procedimientos adecuados, que resalten el papel de las personas como el primer eslabón de una compleja cadena de responsabilidades y que este orientado a preservar los pilares fundamentales de la seguridad de la información:

CONFIDENCIALIDAD: La información debe ser accesible solo a aquellas personas autorizadas.

INTEGRIDAD: La información y sus métodos de procesamiento deben ser completos y exactos.

DISPONIBILIDAD: La información y los servicios deben estar disponible cuando se le requiera.

Para ello es necesario considerar aspecto tales como:

Autenticidad: Los activos de información los crean, editan y custodian usuarios reconocidos quien es validan su contenido.

Posibilidad de auditoria: se mantienen evidencias de todas las actividades y acciones que afectan a los activos de información.

Protección a la duplicación: los activos de información son objeto de clasificación, y se confidenciales.

No repudio: los autores, propietarios y custodios de los activos de información se pueden identificar plenamente.

Legalidad: los activos de la información cumplen los parámetros legales, normativos y estatuarios de la entidad territorial.

Confiablidad de la información: es fiable el contenido de los activos de la información que conserven la confidencialidad, integridad, disponibilidad, disponibilidad, autenticidad y legalidad.

El modelo de seguridad de la información de la alcaldía municipal de puerto Colombia reúne el conjunto de lineamientos, políticas, normas, procesos e instituciones que proveen y promueven la apuesta en marcha, supervisión, mejora y control de la implementación de la estrategia de gobierno digital definida en manual. El modelo está basado en lo expuesto y referenciado por el sistema de administración de seguridad de la información de gobierno digital (SASIGEL).

VISION ESTRATEGICA

La estrategia de gobierno digital contribuye con la construcción de un estado más eficiente, más transparente y participativo y que presta mejores servicios con la colaboración de toda la sociedad, mediante el aprovechamiento de las tecnologías de la información y comunicaciones. Lo anterior con el fin de impulsar la competividad y el mejoramiento de la calidad de vida para prosperidad de todos los colombianos.

Para lograr esta visión nacional, se han adoptado, igualmente, los objetivos:

Facilitar la eficiencia y colaboración en y entre las entidades y dependencia del municipio, así como con la sociedad en su conjunto.

Fortalecer las condiciones para el incremento de la competividad y el mejoramiento de la calidad de vida.

Contribuir al incremento de la transparencia en la gestión pública.

Promover la participación ciudadana haciendo uso de los medios electrónico.

ARQUITECTURA DE GOBIERNO DIGITAL

La arquitectura está compuesta de tres componentes; una red de servicios, un entorno de colaboración y un componente de Gobernabilidad.

La red de servicios, contiene una serie de servicios interrelacionado de información, transacción y participación los cuales son accedidos a través de diferentes canales de acceso, entre los canales de acceso que se puede encontrar están la televisión el internet el celular las canales presenciales entre otras

Los servicios de información corresponden a aquellos servicios que se general exclusivamente para publicar información. Entre los servicios de información encontramos el portal único de contratación, los portales territoriales, los portales de las entidades, entre otros.

Los servicios de transacción corresponden a aquellos servicios sobre los cuales los clientes pueden realizar operaciones en el estado. Entre estos servicios encontramos la ventanilla única de registro de propiedad de inmueble, el certificado de antecedentes fiscales, la solicitud de constancia juramentada por pérdida, extravío de documentos o elementos, entre otros.

Los servicios de participación corresponden a aquellos que dispone el gobierno para promover la participación ciudadana en la toma de decisiones. Entre estos servicios se encuentra la urna de cristal, el micro sitio de vive gobierno digital, entre otros.

El entorno de colaboración es el lugar donde interactúan todos los actores de la sociedad en la construcción de los servicios que serán prestados en la red de servicios. En este entorno se pueden identificar ciudadanos, empresas del sector productivo, entidades del estado y la academia. Este entorno de colaboración da origen a un proceso continuo de publicación de datos, publicados por las entidades, generación de procesos de negocio que hacen uso de estos datos, por parte de todos los actores, esquemas co-creacion, que permiten la interacción de múltiples actores de la sociedad para la prestación de los servicios, en donde cada actor define como prestar el servicio que va a colocar en la red de servicios. Adicionalmente, este proceso se retroalimenta a partir de la participación de los usuarios, desde la mejora a la calidad de los permanentes que promueve la publicación de más datos que a su vez conllevan a la prestación de más servicios.

En el entorno de colaboración los diferentes actores interactúan de la siguiente manera:

Entidades: requieren transformase para poder integrar a los diferentes actores de la sociedad en la prestación de servicios.

Academia: participa entregando conocimientos a partir de sus investigaciones de sobre los actores de la sociedad.

Cuidadnos: participa a través de la creación de comunidades para la participación y construcción colectiva.

Este entorno de colaboración se soporta en unos componentes de apoyo que involucran tanto soluciones de soporte como de infraestructura tecnología.

Las soluciones de soporte corresponden a aquellas soluciones que se requieren por uno o varios servicios, y que faciliten la dinámica del entorno de colaboración al facilitar la concentración de esfuerzos en la construcción de funciones de valor para los clientes. Entre las soluciones de soporte encontramos la solución e3 autenticación en línea, notificación en línea, botón de pago, tramitador en línea. Estas soluciones pueden ser provistas tanto por entidades del estado, como por terceros y dependerá de su uso estratégico quien las desarrolle.

La infraestructura tecnológica corresponde a la base tecnológica sobre la cual operaran los servicios, entre los componentes de la infraestructura tecnológica encontramos centros de datos, redes de comunicación centros de contacto. Cada uno de estos componentes puede ser prestado por varias entidades o empresas, y debe cumplir con un conjunto de estándares de calidad, prestación de servicio y seguridad, que hacen parte de la gobernabilidad.

Finalmente, se encuentran en este componente de apoyo, los esquemas de incentivos, acompañamiento y medición, los cuales facilitan la masificación de la estrategia y la construcción del entorno de colaboración.

El componente de gobernabilidad facilita que la construcción de la arquitectura se puede realizar por parte de todos los actores de la sociedad, a partir de unos principios, lineamientos, metodologías, guías y estándares, así como con la administración de la base de conocimiento y la revisión permanente del marco legal y regulatorio.

RELACION MODELO DE SEGURIDAD

Desde el punto de vista de seguridad, el modelo que se plantea en este documento busca ayudar a la entidad a la provisión del servicio confiable a los clientes, a a partir de unos procesos con los que se pueda crear, distribuir y manipular información electrónica masiva, protegiendo la información electrónica masiva, protegiendo la información del individuo. Para esto, se ha contemplado también sé que desarrolle entre otras, competencias relacionadas con seguridad en la creación de cultura digital que aprovecha las TIC para crear valor a los clientes y se generan capacidades de colaboración entre los funcionarios de las diferentes entidades para poder implementar de manera más eficiente el modelo.

Por lo tanto, el modelo de seguridad se involucra dentro de la arquitectura como un principio, que debe regir todo lo que se construya, y a partir de allí se entregan una serie de

lineamientos, metodologías, guías y estándares, que están al servicio de las entidades para la implementación de la estrategia, e incluyen:

Lineamientos:

- Organigrama del modelo y sistema de atención de seguridad de información de gobierno digital
- Estratificación de entidades
- Control de seguridad
- Indicadores de seguridad.
- Lineamientos para la implementación del modelo de seguridad de la información.

Metodologías:

- Metodología para la gestión de riesgos
- Metodología de clasificación de activos.

Guías:

- Encuesta de seguridad.
- Autoevaluación de entidades, para el análisis de brecha
- Planilla la política de seguridad del sistema de gestión de seguridad de la información – SGSI para las entidades.
- Ejemplos de procedimientos estadales usados.
- Guías de implementación de política.

Finalmente, se incluye una serie de recomendaciones en cada uno de los componentes de la arquitectura, relacionados en la red de servicios y el entorno de colaboración.

SISTEMA DE ADMINISTRACION DE SEGURIDAD DE LA INFORMACION DE GOBIERNO DIGITAL – SASIGEL

Sistema Administrativo de Seguridad de la Información para Gobierno Digital

El modelo de seguridad de la información para las entidades del Estado, se apoya en la creación del sistema administrativo de seguridad de la información para Gobierno Digital – SASIGEL y en la conformación de la comisión de seguridad de la información para Gobierno digital, para tomar acciones estratégicas y definir los lineamientos que permitan la implementación, seguimiento y mantenimiento del modelo de seguridad de la información en cada una de las entidades públicas de orden nacional y territorial y en las entidades privadas que sean proveedoras de los servicios de gobierno Digital.

La creación del sistema administrativo de seguridad de la información para Gobierno Digital, permite el cumplimiento de los principios definidos en la ley 1341 de 2009 y en la estrategia de gobierno digital, que corresponden a la protección de la información del individuo y la credibilidad y confianza en el Gobierno digital.

En particular, para lograr el cumplimiento de estos principios, se requiere que tanto los servicios de Gobierno Digital, como la intranet gubernamental Municipal y las entidades que participen en la cadena de prestación de los servicios de Gobierno digital, cumplan con los tres elementos fundamentales de la seguridad de la información: disponibilidad de la información y los servicios; integridad de la información; y, confidencialidad de la información. Para la correcta administración de la seguridad de la información, se deben establecer y mantener programas y mecanismos que busquen cumplir con los tres requerimientos mencionados.

El SASIGEL surge, como la necesidad de dirigir las interacciones de los actores públicos, privados y de la sociedad civil interactúan y afectan la seguridad de la información de las entidades públicas.

ESTRUCTURA INSTITUCIONAL

La estructura institución, de la figura 4, toma las funciones de rector del modelo, fijado en el modelo nacional, se encuentran en el capítulo tres (3) del anexo No. 1 – organigrama modelo y SASIGEL. Esta estructura garantiza el mantenimiento y sostenibilidad del Modelo de Seguridad de la información en el tiempo, así como su correcta implementación.

APROXIMACION POR PROCESOS PARA SASIGEL

El sistema administrativo de seguridad de la información para gobierno digital, adopta un enfoque basado en procesos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el modelo de seguridad de la información para la estrategia de gobierno digital, orientado hacia todas las entidades y los actores involucrados.

La aproximación se hacer a través del modelo PHVA de la figura, donde se identifican las diferentes etapas como son la planeación y publicación del modelo, el hacer, con la ambientación de las entidades y dependencias municipales, formación de capacitadores e implementación de SGSI en las entidades y dependencias, este último desarrollado en detalle en un capítulo más adelante…el verificar mediante el seguimiento y control. Y el actuar mediante la revisión y mejoras al modelo.

POLITICA DE SEGURIDAD DE LA INFORMACION

La información es un recurso que como el resto de los activos tienen valor para la entidad y por consiguiente debe ser debidamente protegida. El establecimiento, seguimiento, mejora continua y aplicación de la política de seguridad de la información garantiza un compromiso ineludible de protección a la misma frente a una amplia gama de amenazas. Con esta política se contribuye a minimizar los riesgos asociados de daño y sea segura el eficiente cumplimiento de las funciones sustantivas de la entidad apoyadas en un correcto del sistema de información.

En la ALCALDIA MUNICIPAL DE PUERTO COLOMBIA la información es un activo fundamental para prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la administración de riesgos y la consolidación de una cultura de seguridad.

Consciente de sus necesidades actuales la ALCALDIA MUNICIPAL DE PUERTO COLOMBIA implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios vigentes.

El proceso de análisis de riesgos de los activos de información es el soporte para el desarrollo de las políticas de seguridad de la información y de los controles objetivos en la alcaldía municipal e puerto Colombia; este proceso será liderado de manera permanente por comité designado para tal fin.

Esta política será revisada con regularidad como parte del proceso de revisión estratégica, o cuando se identifiquen cambios en la entidad, su estructura, sus objetivos o alguna condición que afecte la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados.

La ALCALDIA MUNICIPAL DE PUERTO COLOMBIA, para el cumplimiento de su misión, visión, objetivo estratégico y apegado a sus valores corporativos, establece la función de seguridad de la información en la entidad con el objetivo de:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información

- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes.
- Garantizar la continuidad del negocio frente a incidentes.

POLITICAS GENERALES DE SEGURIDAD DE LA INFORMACION

- La ALCALDIA MUNICIPAL DE PUERTO COLOMBIA, ha decidido definir, implementar, operar y mejorar de forma continua un sistema de gestión de seguridad de la información, soportado en lineamientos claros, alineados a las necesidades de la entidad, y a los requerimientos regulatorio. Las responsabilidades frente a la seguridad de la información serán definidas, compartida, publicadas y aceptadas por cada uno de los empleados, proveedores o terceros.
- La ALCALDIA MUNICIPAL DE PUERTO COLOMBIA protegerá la información generada, procesada o resguardada por los procesos estratégicos, misionales y de apoyo a la entidad, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej: proveedores o clientes), o como resultado de un servicio interno en oitsourcing.
- La ALCALDIA MUNICIPAL DE PUERTO COLOMBIA protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocios, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto d esta. Para ellos es fundamental la aplicación de controles de acuerdos con la clasificación de la información de su propiedad o en custodia.
- La ALCALDIA MUNICIPAL DE PUERTO COLOMBIA protegerá su información de las amenazas originadas por parte del personal.
- La ALCALDIA MUNICIPAL DE PUERTO COLOMBIA protegerá las instalaciones de procesamientos y la infraestructura tecnológica que soporta sus procesos críticos.
- La ALCALDIA MUNICIPAL DE PUERTO COLOMBIA controlara la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La ALCALDIA MUNICIPAL DE PUERTO COLOMBIA implementara control de acceso a la información, sistemas y recursos de red.
- La ALCALDIA MUNICIPAL DE PUERTO COLOMBIA garantizara que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La ALCALDIA MUNICIPAL DE PUERTO COLOMBIA garantizara a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectivo de su modelo de seguridad.

- La ALCALDIA MUNICIPAL DE PUERTO COLOMBIA garantizara la disponibilidad de sus procesos de negocio y continuidad de sus operaciones basada en el impacto que pueden generar los eventos
- La ALCALDIA MUNICIPAL DE PUERTO COLOMBIA garantizara el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.
- La ALCALDIA MUNICIPAL DE PUERTO COLOMBIA definirá e implementará controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la entidad.

POLITICAS, CONTROLES Y PROCEDIMIENTOS

COMPUTADORES, PORTATILES Y SERVIDORES

Políticas

- Los mecanismos de control de acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas de La ALCALDIA MUNICIPAL DE PUERTO COLOMBIA solo a personas autorizadas para la salvaguarda de los equipos de cómputo y de comunicaciones.
- Los computadores de la compañía solo deben usarse en ambiente seguro. Se considera que un ambiente seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.

Controles

- El usuario deberá reportar de forma inmediata al área de sistemas cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, conatos de incendio u otro.
- El usuario tiene la obligación de proteger las unidades de almacenamiento que se encuentran bajo su administración, aun cuando no se utilicen y contengan información reservada y confidencial.
- Es responsabilidad del usuario evitar en todo momento la fuga de la información de la institución que se encuentra almacenada en los equipos de cómputo personal que tenga asignados.
- Cualquier persona que tenga acceso a las instalaciones de la Alcaldía Municipal de Puerto Colombia.