ALCALDÍA MUNICIPAL DE CHÍA

Oficina de Tecnologías de la Información y las Comunicaciones, TIC

Política de Seguridad Digital 2020-2023

(Versión 1)

ALCALDÍA MUNICIPAL DE CHÍA

Cra. 11 No 11 - 29
PBX: 8844444 Ext. 2300
oficinatic@chia.gov.co
www.chia-cundinamarca.gov.co

Tabla de contenido

Cra. 11 No 11 - 29
PBX: 8844444 Ext. 2300
oficinatic@chia.gov.co
www.chia-cundinamarca.gov.co

POLÍTICA DE SEGURIDAD DIGITAL

1. Contexto de la política

¿Qué es?

El constante aumento en el uso de las Tecnologías de la Información y las Comunicaciones (TICs) en Colombia, en campos sociales, económicos y educativos ha generado grandes oportunidades de crecimiento y formación como ciudadanos digitales, tanto así, que ha permitido aumentar las capacidades de interacción entre la población y las entidades de orden nacional y territorial, permitiendo ampliar catálogos de servicios y atención a las problemáticas de la población, generando de igual manera trámites y servicios de calidad a través de plataformas digitales como las Ventanillas Únicas Virtuales. Esto ha generado oportunidades y avance en todo tipo de actividad digital, lo que también logra generar riesgos de todo tipo en seguridad digital, afectando la integridad de los datos tanto de las entidades públicas, como datos de la población (información personal) que interactúa con estas.

Es en este punto en donde se busca generar lineamientos que reduzcan los riesgos a nivel de seguridad digital que se generen en estos nuevos contextos de avance en el uso de las TICs.

¿Para qué sirve?

Permite realizar actividades de mitigación y eliminación de cualquier tipo de riesgo digital que pueda afectar la confianza de los ciudadanos digitales y la calidad de datos que se gestionan por ambas partes. Es así que se debe encaminar una Política de Seguridad Digital que permita contrarrestar cualquier amenaza cibernética y mitigue todo tipo de riesgo, teniendo presente directrices y recomendaciones en el CONPES 3854 de Seguridad Digital, adicionando aspectos del Decreto Nacional 1078 de 2015 y del Modelo de Privacidad de la Información (MSPI) expedido por el MinTIC.

En el presente documento contiene la formulación de la Política de Seguridad Digital para el municipio de Chía, diseñado bajo lineamientos del Modelo Integrado de Planeación y Gestión – MIPG, en el marco de su implementación.

¿Con qué otras políticas de gestión y desempeño se articula?

- Transparencia, acceso a la información pública y lucha contra la corrupción.
- Gobierno Digital
- Seguridad de la información

Objetivo General

Diseñar la Política de Seguridad Digital de la Alcaldía Municipal de Chía orientada a la identificación, gestión y mitigación de riesgos de seguridad digital para la generación de confianza de los ciudadanos digitales en el municipio.

Objetivos Específicos

- Establecer lineamientos para una correcta gestión del riesgo de seguridad digital en actividades propias de la entidad.
- Capacitar a los funcionarios de la Alcaldía Municipal de Chía en buenas prácticas digitales.
- Desarrollar confianza digital a través de la mejora de la seguridad digital en la entidad.
- Fortalecer la capacidad de la Alcaldía Municipal de Chía en materia de prevención de riesgos digitales.

Glosario

La mayoría de las definiciones se toman de la Política Nacional de Confianza y Seguridad Digital – CONPES 3995.

- **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:** posible violación de la seguridad digital que tiene el potencial de ocurrir total o parcialmente en el entorno digital. Se caracteriza por la aparición de una situación donde uno o más actores (externos o internos) adelantan una o varias acciones con la capacidad de alterar una

infraestructura física, un sistema de información o la integridad de la información en sí.

- **Ataque:** amenaza intencional que se concreta.
- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Ciberdefensa:** capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. La ciberdefensa implica el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética.
- **Ciberdelincuencia:** conjunto de acciones y actividades ilícitas que son cometidas total o parcialmente en el entorno digital, asociadas con el uso de las Tecnologías de la Información y las Comunicaciones o la utilización de un bien o servicio informático con el fin de causar daño, generar problemas o adelantar una agresión cibernética con el objetivo del propio beneficio o para desestabilizar la población, el territorio y la organización política del Estado.
- **Ciberdelito / Delito cibernético:** actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito. (Ministerio de Defensa de Colombia)
- **Ciberespacio:** es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Ciberseguridad:** se entiende como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética, buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio de las interacciones digitales. La ciberseguridad tiene el fin de proteger a los usuarios y los activos de Estado en el Ciberespacio y comprende el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para dicho fin.

- **Dato:** Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
- **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.
- **Entorno digital:** ambiente, tanto físico como virtual sobre el cual se soportan las interacciones del futuro digital, tales como la economía digital.
- **Incidente:** cualquier evento adverso real o sospechado, intencionado o no intencionado, que puede cambiar el curso esperado de una actividad en el entorno digital.
- **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.
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Riesgo:** es el efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas.
- **Riesgo informático:** posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. (ISO Guía 73:2002)
- **Seguridad digital:** es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante la gestión del riesgo de seguridad digital; la implementación efectiva de medidas de ciberseguridad; y el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.
- **Vulnerabilidad:** es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan.

Cra. 11 No 11 - 29
PBX: 8844444 Ext. 2300
oficinatic@chia.gov.co
www.chia-cundinamarca.gov.co

¿Cuáles son sus fundamentos normativos?

NORMATIVIDAD ASOCIADA
NORMAS NACIONALES
Ley 1150 de 2007 Ley 1341 de 2009 Ley 1273 de 2009 Ley 1474 de 2011 Ley 1581 de 2012 Ley 1712 de 2014 Ley 2052 de 2020 Resolución 3564 de 2015 Resolución 2710 de 2017 Resolución 1519 del 2020 Resolución 1126 de 2021 Directiva No. 02 de abril de 2019 Decreto 612 del 4 de abril de 2018 Decreto 1413 de 2017 Decreto 2693 de 2012 Decreto 212 de 2014 Decreto 1078 de 2015 Decreto 612 de 2018 Decreto 2106 de 2019 Decreto 620 de 2020 Decreto 1692 de 2020 Acuerdo 03 de 2015 del AGN CONPES 3995
NORMAS TERRITORIALES
Acuerdo 168 de 2020 (Plan de Desarrollo Municipal)

¿Cuál es la estructura o elementos de la política?

Para la presente política se tendrá en cuenta la metodología establecida en la política de administración de riesgos de seguridad de la información vigente en la entidad, la cual se basa en la norma NTC-ISO/IEC 27005 (véase figura 1)

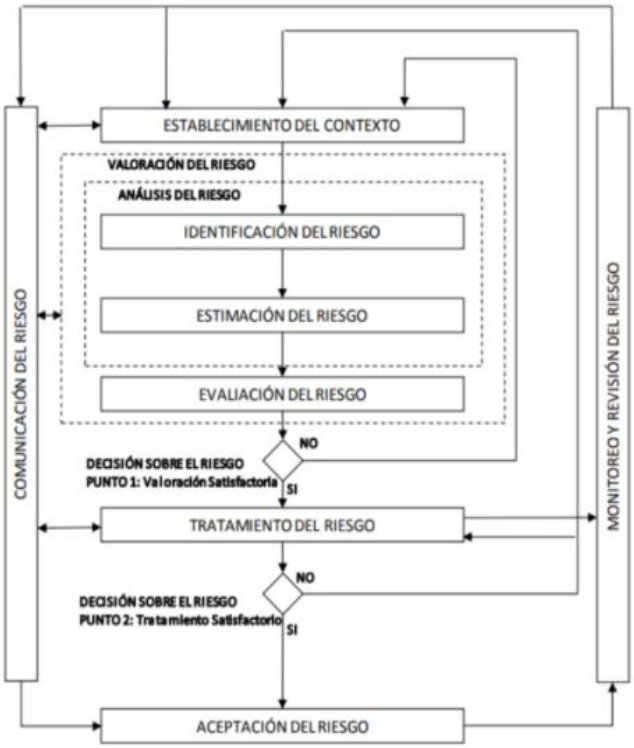

Ilustración 1 Administración del riesgo

La Política de Seguridad cuenta con los siguientes lineamientos aplicables a todas las áreas de la Alcaldía Municipal de Chía:

- La Oficina de Tecnologías de la Información y las Comunicaciones se encargará de definir, actualizar y socializar lineamientos sobre seguridad digital de manera anual.

- La Oficina de Tecnologías de la Información y las Comunicaciones debe designar un responsable de seguridad digital quien también es responsable de la seguridad de la información. La persona designada tendrá las siguientes responsabilidades frente a la seguridad digital de la entidad:
    - Definir el procedimiento para la identificación y valoración de Activos.
    - Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento).
    - Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos.
    - Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
    - Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.
- De manera anual en la Alcaldía Municipal de Chía se deberá realizar la actualización y documentación de activos de información, se categorizará y se valorará cada activo según lo defina el responsable de seguridad digital.
- La identificación de activos de información se deberá realizar teniendo en cuenta los pasos establecidos en el “Anexo 4 – Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas”, el cual lo define de la siguiente manera:
    - Listar los activos por cada proceso.
    - Identificar el dueño o responsable de los activos.
    - Clasificar los activos.
    - Clasificar la información.
    - Determinar la criticidad del activo.
    - Identificar si existen infraestructuras cibernéticas.
- Cada jefe de oficina se encargará de socializar la política de seguridad digital a su equipo de trabajo y definirá un encargado para hacer el seguimiento y cumplimiento de la misma.
- La Oficina de Tecnologías de la Información y las Comunicaciones verificará que todo desarrollo y plataforma digital propia, cumpla con los estándares de seguridad y protección de la información.

- Se deben aplicar controles de acuerdo con la clasificación de la información salvaguardada y custodiada por cada uno de los funcionarios, minimizando impactos financieros, operativos o legales debido a un mal uso de esta.
- Toda información que adquiera la Alcaldía Municipal de Chía de manera externa deberá ser analizado con el antivirus institucional vigente.
- El uso de la información de cada equipo de la entidad será responsabilidad del funcionario asignado.
- Para el acceso a los servicios de red (corrycom, ventanilla única, correo electrónico, etc) se entrega usuario (correo electrónico institucional) y contraseña, la cual debe ser cambiada por el usuario propietario del acceso y ser de uso exclusivo e intransferible. La confidencialidad de las contraseñas de acceso será de responsabilidad del funcionario.
- Cualquier funcionario y/o contratista que requiera capacitación en la administración del paquete de herramientas de G-Suite del correo institucional para temas de teletrabajo, deberá realizar la solicitud de manera formal a la Oficina de Tecnologías de la Información y las Comunicaciones.
- La Oficina de Tecnologías de la Información y las Comunicaciones será la encargada de hacer seguimiento a las aplicaciones instaladas en los equipos de cómputo de la entidad, verificando que cumplan con los estándares de uso bajo licenciamiento.
- Se debe evitar la divulgación, modificación, retiro o destrucción no autorizada de información almacenada en los dispositivos móviles propios de la entidad.
- Toda información de la entidad que se gestione de manera remota (teletrabajo) deberá ser salvaguardada en el drive del correo institucional.
- Hangouts Meet será la herramienta recomendada para la realización de reuniones de manera virtual, esta herramienta se encuentra disponible en el paquete de herramientas de G-Suite del correo institucional, según el tipo de licencia asignada a cada usuario.
- Se debe minimizar el uso de dispositivos extraíbles dentro de la entidad para prevenir la infección de los equipos de cómputo de la entidad. Se debe aprovechar herramientas alternas como el almacenamiento en la nube del correo institucional (Google Drive) el cual, según la licencia asignada, tiene una capacidad de 30 GB, ó 2TB, compartidas.
- Todos los funcionarios y contratistas serán los responsables de salvaguardar información relevante de sus procesos para evitar accesos no autorizados, robo de información y realizar respaldos periódicos de la misma.

- Todos los funcionarios, ya sean contratistas o de planta, deben realizar la entrega de la información trabajada en el desempeño de sus labores y backup del correo electrónico a su jefe inmediato y una vez realizada la entrega de la información debe tramitar ante la oficina TIC liberación de la licencia de correo, para la emisión del respectivo paz y salvo.
- Todos los funcionarios y contratistas de la entidad deberán reportar a la Oficina de Tecnologías de la Información y las Comunicaciones cualquier actividad que pueda atentar de manera directa o indirecta la integridad de la información que se gestiona en las actividades laborales.
- Todos los funcionarios y contratistas de la entidad deberán reportar a la Oficina de Tecnologías de la Información y las Comunicaciones cualquier actividad sobre mal uso de las herramientas TIC a su disposición, ya sea mal uso del internet para acceso a páginas web no permitidas, divulgación de correos de procedencia dudosa, entre otros casos que puedan afectar la seguridad digital de la entidad.

¿Cuál es su ámbito de aplicación?

Para la implementación de la política de seguridad digital en la Alcaldía Municipal de Chía, el líder será la Oficina de Tecnologías de la Información y las Comunicaciones. De igual manera, para el debido cumplimiento, todas las dependencias serán corresponsables de las acciones o información requeridas por el líder de política para su monitoreo, medición y seguimiento.

¿Quiénes la ejecutan?

a) Responsable de liderar la implementación de la política a nivel territorial.
b) Representante legal y nivel directivo.
c) Funcionarios y contratistas de la entidad.

2. ¿Cómo se planea la política?

- Plan de Desarrollo Municipal: Instrumento de planificación que orienta las acciones de la administración municipal durante un período de gobierno. En éste se determina la visión, los programas, proyectos y metas de desarrollo

asociados a los recursos públicos que ejecutarán durante los próximos 4 años.

- Plan indicativo: Es un instrumento que permite resumir y organizar por anualidades los compromisos asumidos por el alcalde en el plan de Desarrollo. En él se precisan los resultados y productos que se esperan alcanzar en cada vigencia y al terminar el periodo de gobierno.

- Plan de acción: Es un instrumento que sirve para que cada una de las dependencias oriente sus procesos, instrumentos y recursos disponibles (humanos, financieros, físicos, tecnológicos e institucionales) hacia el logro de sus objetivos y metas anuales de la Administración.

3. ¿Cómo se implementa la política?

Para cumplir con los objetivos de la Política de Seguridad Digital en la alcaldía Municipal de Chía se contemplan las siguientes líneas estratégicas:

- Estructura administrativa y direccionamiento estratégico: Compromiso de la Alta Dirección e institucionalidad formal para el cumplimiento de la política de seguridad digital.

- Fortalecimiento de capacidades: Capacitación y campañas de sensibilización sobre el uso correcto de las TICs, identificación, clasificación y mitigación de riesgos de seguridad digital.

- Normativo y procedimental: Elaboración y/o actualización de los protocolos y documentación necesaria para el cumplimiento normativo, en temas de tratamiento de datos personales, transparencia y acceso a la información.

Cra. 11 No 11 - 29
PBX: 8844444 Ext. 2300
oficinatic@chia.gov.co
www.chia-cundinamarca.gov.co

4. ¿Qué herramientas están disponibles para su implementación?

Para la correcta implementación de la política de seguridad digital, se tendrá como punto de partida la Política Nacional de Confianza y Seguridad Digital – CONPES 3995 la cual dispone los lineamientos iniciales para la gestión y mitigación de riesgos de seguridad digital en el territorio nacional, de igual manera se presentan las siguientes herramientas de complemento:

- Resultados FURAG 2020
- Plataforma de seguimiento “Resultados de desempeño institucional territorio, vigencia 2020”
- CONPES 3995
- Modelo de Seguridad y Privacidad de la Información – MSPI 2020
- Política de administración de riesgos

5. ¿Cómo se realiza el seguimiento y medición de la política?

Monitoreo y Seguimiento

En primera instancia el Ministerio de Tecnologías de la Información y las Comunicaciones definirá el procedimiento para el seguimiento y evaluación de la Política de seguridad digital en el marco de los lineamientos nacionales.

La oficina de control interno de la entidad será la encargada de realizar seguimiento y evaluación a la política de seguridad digital de acuerdo al plan de acción definido.

Cra. 11 No 11 - 29
PBX: 8844444 Ext. 2300
oficinatic@chia.gov.co
www.chia-cundinamarca.gov.co

Medición:

El Modelo Integrado de Planeación y Gestión cuenta con una herramienta en línea, llamado Formulario Único Reporte de Avances de la Gestión - FURAG, a través del cual se capturan, monitorean y evalúan los avances sectoriales e institucionales en la implementación de las políticas de desarrollo administrativo de la vigencia anterior al reporte.

Elaborado Por:
Ing. Jonathan Sebastián Gómez
Contratista Oficina TIC

Revisado Por:
Ing. Eliany R. Montejo Carrascal
Profesional Especializado Oficina TIC

Aprobado por:
Ing. Jorge Iván Ortiz Ardila
Jefe Oficina TIC