Municipio de Guatapé
Departamento de Antioquia

@alcguatape

2024

Plan de Seguridad y Privacidad de la Información

MUNICIPIO DE GUATAPÉ - ANTIOQUIA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2024

DAVID ESTEBAN FRANCO VALLEJO
Alcalde Municipal

ESTEFANÍA JIMÉNEZ HERRÓN
Secretaria de Turismo y Desarrollo Económico

YEISON DAVID GIRALDO TABARES
Asesor de Ciencia, Tecnología e Innovación

FICHA DEL DOCUMENTO

Titulo:	**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**
Sumario:	Este documento tiene por objeto Desarrollar e implementar el Plan de Seguridad y Privacidad de la Información del Municipio de Guatapé, en busca de salvaguardar la confidencialidad, integridad y disponibilidad de la información en cumplimiento a la normatividad vigente y el aseguramiento de la información como el activo más significativo de la entidad
Palabras claves:	Seguridad, Privacidad, Confidencialidad, Gobierno Digital, Municipio de Guatapé. riesgos
Formato:	PDF
Dependencia:	TIC – Secretaría de Turismo
Autor (es):	Yeison David Giraldo Tabares
Revisó:	Estefanía Jiménez Herrón
Fecha de Aprobación:	29 de enero de 2024
Versión aprobada:	4.0
Idioma	Español

CONTENIDO

1. INTRODUCCIÓN

La seguridad de la información está basada en la tecnología y promueve la confidencialidad de la misma: la información está centralizada y puede tener un alto valor, pero también puede ser divulgada, mal utilizada, además involucra realizar un análisis de riesgos para conocer las posibles fuentes de amenazas que puedan atentar contra la disponibilidad, la integridad, confidencialidad, o bien genera un rechazo de información. (UNAM, 2004)

En tal sentido, se diseña e implementará el presente Plan de Seguridad y Privacidad de la Información para garantizar la confidencialidad, disponibilidad e integridad de la información, principios fundamentales de un Sistemas de Seguridad y Privacidad de la Información.

También para el diseño del Plan se tiene en cuenta la Política de Gobierno Digital que ha definido dos componentes: TIC para el Estado y TIC para la Sociedad. Estos componentes permiten mejorar el funcionamiento de las entidades públicas, su relación con otras entidades y el fortalecimiento de su relación con la sociedad.

Ilustración 1 Política de Gobierno Digital - Fuente MINTIC

2. JUSTIFIACIÓN

La seguridad de la información se define como un proceso integrado que permite proteger la identificación y gestión de la información y los riesgos a los que esta se puede ver enfrentada, en tal sentido el Plan de seguridad y privacidad de la Información contribuye a que el Municipio de Guatapé, incremente los niveles de confidencialidad, integridad y disponibilidad de la información fomentando una cultura institucional, en cuanto a la necesidad de preservar los activos de información de la Entidad, en cumplimiento a lo definido en la Línea: Guatapé emprende por la Gobernanza, seguridad y buen gobierno, Componente: Fortalecimiento Institucional, Programa: Fortalecimiento de procesos administrativos el cual tiene como uno de sus objetivos fortalecer la capacidad administrativa y organizacional, así como los procesos para prestar un servicio a la comunidad ágil, oportuno y eficiente.

3. ALCANCE

El Plan de Seguridad y Privacidad de la Información contempla los controles definidos en la Norma Técnica Colombia ISO IEC 27001:2013, mediante el cual se busca la implementación de buenas prácticas para salvaguardar toda la información del Municipio de Guatapé y comprometer a los funcionarios y contratistas en la adopción y apropiación de medidas de seguridad de la información.

4. OBJETIVOS

4.1 General

Desarrollar e implementar el Plan de Seguridad y Privacidad de la Información del Municipio de Guatapé, en busca de salvaguardar la confidencialidad, integridad y disponibilidad de la información en cumplimiento a la normatividad vigente y el aseguramiento de la información como el activo más significativo de la entidad.

4.2 Objetivos Específicos

- ✓ Elaborar la Política de Seguridad y Privacidad de la Información
- ✓ Diseñar e implementar el Modelo de Seguridad y Privacidad de la Información
- ✓ Velar por la implementación de las políticas sobre seguridad digital elaboradas por la entidad.
- ✓ Formular e implementar un plan de Capacitaciones para los funcionarios y contratistas de la entidad sobre la importancia de conservar la seguridad y privacidad de la información institucional y preservar los activos de información.
- ✓ Diseñar plan de acción en caso de pérdida de la información por desastre natural, siniestro o ataque informático.

5. MARCO NORMATIVO

MARCO NORMATIVO	AÑO	DESCRIPCIÓN
Resolución 0500 de 2021	2021	Por la cual se establece los lineamientos y estándares para la estrategiade seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de gobierno digital
LEY 1978 de 2019	2019	Por la cual se moderniza el sector de las tecnologías dela información y las comunicaciones -TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones”
LEY 1955 de 2019	2019	Por la cual se expide el Plan Nacional de Desarrollo, en los artículos 147 y 148 se establece lo referente a la Transformación Digital Pública yGobierno Digital como política de gestión y desempeño Institucional”
Decreto 1008	2018	Por el cual se establecen los lineamientos generales de lapolítica de Gobierno Digital.
CONPES 3854 del 2016	2016	Por el cual establece la Política Nacional de Seguridad Digital”
Decreto 1083 de 2015	2015	Se insta a las entidades públicas a realizar acciones tendientes para quelos proyectos de Transformación Digital se integren a los planes institucionales y estratégicos, incluyendo el Plan Estratégico de Tecnología y Sistemas de Información (PETI), EL Plan de Seguridad y Privacidad de la Información y el Plan de Tiramiento de Riesgos de Seguridad y Privacidad de la información en el marco de la Política de Gobierno Digital.

Decreto 1078 de 2015	2015	*Por medio del cual se expide el Decreto Único Reglamentario del Sectorde Tecnologías de la Información y las Comunicaciones*
Ley 712 de 2014	2014	Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional. Se regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.
Decreto 2573 de 2014	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 sedictan otras disposiciones

6. GLOSARIO

- ✓ **Acceso a la Información Pública**: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y accedera la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- ✓ **Activo de Información**: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere,obtenga, adquiera, transforme o controle en su calidad de tal.
- ✓ **Amenazas** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- ✓ **Análisis de Riesgo** Proceso para comprender la naturaleza del riesgo ydeterminar el nivel de riesgo. (ISO/IEC 27000).
- ✓ **Bases de Datos Personales**: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
- ✓ **Ciberseguridad**: Capacidad del Estado para minimizar el nivel de riesgo al queestán expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- ✓ **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).
- ✓ **Datos Abiertos**: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales

están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

- ✓ **Datos Personales**: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- ✓ **Datos Personales Públicos**: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comercianteo de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)
- ✓ **Datos Personales Privados**: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
- ✓ **Datos Personales Mixtos**: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
- ✓ **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 garantíasde partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)
- ✓ **Gestión de incidentes de seguridad de la información:** Procesos paradetectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- ✓ **Información Pública Clasificada**: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbitopropio, particular y privado o semiprivado de una persona natural o jurídica porlo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- ✓ **Información Pública Reservada**: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de accesoa la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos

consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6) • Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266de 2008.

- ✓ **Ley de Transparencia y Acceso a la Información Pública**: Se refiere a la Ley Estatutaria 1712 de 2014.
- ✓ **Mecanismos de protección de datos personales**: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protecciónа los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
- ✓ **Privacidad**: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- ✓ **Registro Nacional de Bases de Datos**: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)
- ✓ **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 consecuencias. (ISO/IEC 27000).
- ✓ **Seguridad de la información**: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- ✓ **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, basándoseen un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- ✓ **Tratamiento de Datos Personales**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- ✓ **Trazabilidad**: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

7. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

La seguridad informática consiste en la implementación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, lo que conlleva a mantener un sistema seguro y fiable.

7.1 Confidencialidad: para garantizar que la información sólo sea accesible para las personas autorizadas a tener acceso, prevenir la divulgación no autorizada de la información sobre nuestra organización.

7.2 Integridad: para salvaguardar la exactitud y la exhaustividad de la información y los métodos de tratamiento, supone que la información se mantenga inalterada ante accidentes o intentos maliciosos. Sólo se podrá modificar la información mediante autorización.

7.3 Disponibilidad: busca garantizar que los usuarios autorizados tengan acceso a la información y a los activos asociados cuando sea necesario. supone que el sistema informático se mantenga trabajando sin sufrir ninguna degradación en cuanto a accesos. Es necesario que se ofrezcan los recursos que requieran los usuarios autorizados cuando se necesiten. La información deberá permanecer accesible a elementos autorizado.

8. ACTIVIDADES A DESARROLLAR

Con el fin de dar cumplimiento a los objetivos planteados en el presente plan, se propones 6 actividades con su respectivo responsable y tiempo de ejecución.

No	ACTIVIDAD	RESPONSABLE	FECHA DE INICIO	FECHA FIN	RECURSOS BIBLIOGRAFICOS	ENTRAGABLE
1	Elaborar e implementar la política de Seguridad y Privacidad de la Información	Asesor de ciencia, tecnología e innovación	01/02/ 2024	30/06/ 2024	MINTIC. Elaboración de la Política general de seguridad y privacidad de la información, guía nro 2, 2016	Política de Seguridad y Privacidad de la Información implementada

2	Verificar nivel de implementación, socializar y velar por el cumplimientode la política de Seguridad Digital	Asesor de ciencia, tecnología e innovación	01/04/ 2024	31/12/ 2024	Municipio de Guatapé. Políticade seguridad Digital, 2022	Política de Seguridad Digital implementada
3	Verificar nivel de implementación, socializar y velar por el cumplimientode política de gobierno Digital	Asesor de ciencia, tecnología e innovación	01/04/ 2024	31/12/ 2024	Municipio de Guatapé. Políticade Gobierno Digital, 2022	Política de Gobierno Digital implementada
4	Verificar nivel de implementación, socializar y velar por el cumplimientode la política de Transparencia y Acceso a la Información.	Asesor de ciencia, tecnología e innovación y Área de Comunicaciones	01/04/ 2024	31/12/ 2024	Municipio de Guatapé Transparencia y Acceso a la Información, 2022	Política de Transparencia y Acceso a la Información implementada
5	Documentar e implementar el Modelo de Seguridad y Privacidad de la Información - MSPI	Asesor de ciencia, tecnología e innovación	01/02/ 2023	30/06/ 2024	MINTIC. Modelode Seguridad y Privacidad de laInformación, 2016	Documento con el Modelo de Seguridad y Privacidad de la información.
6	Diseñar e implementar un plan de Capacitación para sensibilizar a los funcionarios y contratistas sobre la importancia de conservar la seguridad y privacidad de la información institucional con enfoque de almacenamiento en la nube.	Asesor de ciencia, tecnología e innovación	15/02/ 2024	30/12/ 2024	Municipio de Guatapé. Plan Institucional de capacitación, 2024	Plan de capacitación diseñado y ejecutado

7	Diseñar un plan de acción en caso de pérdida de la información por desastre natural, siniestro o ataque informático.	Asesor de ciencia, tecnología e innovación	02/02/ 2024	30/06/ 2024	MINTIC. Modelode Seguridad y Privacidad de laInformación, 2016	Documento con el plan de acción.

9. PLAN GENERAL Y DE SEGUIMIENTO

9.1 Indicadores

N°	ACTIVIDAD	INDICADOR	FORMULA	SENTIDO	META
1	Elaborar e implementar la política de Seguridad y Privacidad de la Información	Política de seguridad y privacidad de la información	Cantidad de políticas diseñadas * 100 / Cantidad de políticas a diseñar	Ascendente	100%
2	Verificar nivel de implementación, socializar y velar por el cumplimiento de la Política de Seguridad Digital.	% de implementación de la Política de Seguridad Digital	Cantidad de actividades ejecutadas * 100 / Cantidad de actividades a ejecutar	Ascendente	100%
3	Verificar nivel de implementación, socializar y velar por el cumplimiento de la Política de Gobierno Digital.	% de implementación de la Política de Gobierno Digital	Cantidad de actividades ejecutadas * 100 / Cantidad de actividades a ejecutar	Ascendente	100%
4	Verificar nivel de implementación, socializar y velar por el cumplimiento de la Política Transparencia y acceso a la Información.	% de implementación de la Política de Transparencia y Acceso a la Información	Cantidad de actividades ejecutadas * 100 / Cantidad de actividades a ejecutar	Ascendente	100%
5	Documentar e implementar el Modelo de Seguridad y Privacidad de la	Modelo de seguridad y privacidad de la información	Cantidad de actividades ejecutadas * 100 / Cantidad de actividades a ejecutar	Ascendente	100%

	Información – MSPI	% de implementación del MSPI	Componentes implementados * 100 / Total componentes de MSPI		
6	Diseñar e implementar un plan de Capacitación para sensibilizar a los funcionarios y contratistas sobre la importancia de conservar la seguridad y privacidad de la información institucional con enfoque de almacenamiento en la nube.	Capacitación a funcionarios públicos	# de capacitaciones dadas / Total de capacitaciones planeadas	Ascendente	100%
7	Diseñar un plan de acción en caso de pérdida de la información por desastre natural, siniestro o ataque informático.	% de implementación de las actividades de Backup	Cantidad de actividades ejecutadas * 100 / Cantidad de actividades a ejecutar	Ascendente	100%

9.2 Mapa de Ruta

ACTIVIDADES		2024 (trimestre)			
		I	II	III	IV
1	Elaborar e implementar la política de Seguridad y Privacidad de la Información				
2	Verificar nivel de implementación, socializar y velar por el cumplimiento de la política deSeguridad Digital				
3	Verificar nivel de implementación, socializar y velar por el cumplimiento de la política degobierno Digital				
4	Verificar nivel de implementación, socializar y velar por el cumplimiento de la política deTransparencia y Acceso a la Información				
5	Documentar e implementar el Modelo de Seguridad y Privacidad de la Información - MSPI				

6	Diseñar e implementar un plan de Capacitaciones para sensibilizar a los funcionarios y contratistas sobre la importancia de conservar la seguridad y privacidad de la información institucional				
7	Diseñar un plan de acción en caso de pérdida de la información por desastre natural, siniestro o ataque informático.				

10. REFERENCIAS BIBLIOGRÁFICAS

- Estrategia De Gobierno Digital. Ministerio De Las TIC
- Plan De Tratamiento De Riesgos De Seguridad Y Privacidad De La Información. Decreto 612 De 2018 – DAFP
- Plan de Seguridad Y Privacidad de La Información. Decreto 612 De 2018 – DAFP
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales

CONTROL DE CAMBIOS

Fecha	Versión	Descripción
Enero / 2020	1	Versión inicial del documento
Enero / 2021	2	Actualización de Plan
Enero / 2022	3	Actualización del Plan
Enero / 2023	4	Actualización del Plan
Enero / 2024	5	Actualización del Plan