MSPI

Alcaldía de La Estrella

INTRODUCCION

Hoy en día, la información está definida como uno de los activos más valiosos y primordiales para cualquier tipo de organización, la cual, sólo tiene sentido cuando está disponible y es utilizada de forma adecuada, integra, oportuna, responsable y segura, lo que implica, que es necesario que las organizaciones tengan una adecuada gestión de sus recursos y activos de información con el objetivo de asegurar y controlar el debido acceso, tratamiento y uso de la información.

El aseguramiento y la protección de la seguridad de la información de las organizaciones y de los datos de carácter personal de los usuarios, representan un reto al momento de pretender garantizar su confidencialidad, integridad, disponibilidad y privacidad, razon por la cual, la seguridad de la información se ha convertido en uno de los aspectos de mayor preocupación a nivel mundial.

Cualquier tipo de organización independiente de su tamaño y naturaleza, debe ser consciente que la diversidad de amenazas existentes que actualmente atentan contra la seguridad y privacidad de la información, representan un riesgo que al materializarse no solo les puede acarrear costos económicos, sanciónales legales, afectación de su imagen y reputación, sino que pueden afectar la continuidad y supervivencia del negocio.

Lo anterior, sumando a un entorno tecnológico en donde cada día se hace más complejo de administrar y asegurar, genera que cada vez más la seguridad de la información forme parte de los objetivos y planes estratégicos de las organizaciones.

Por lo tanto, es indispensable que los responsables dentro de las organizaciones encargados de velar por la protección y seguridad de sus recursos, infraestructura e información, contantemente estén adoptando, implementando y mejorando medidas de seguridad orientadas a prevenir y/o detectar los riesgos que pueden llegar a comprometer la disponibilidad, integridad y confidencialidad de los activos de información a través de los cuales se gestiona la información del negocio, independientemente si está es de carácter organizacional o personal, o de tipo pública o privada.

En la medida que las organizaciones tengan una visión general de los riesgos que pueden afectar la seguridad y privacidad de la información, podrán establecer controles y medidas efectivas, viables y transversales con el propósito de salvaguardar la disponibilidad, integridad y confidencialidad tanto de la información del negocio como los datos de carácter personal de sus empleados, usuarios y partes interesadas. Es indispensable que las organizaciones realicen una adecuada identificación, clasificación, valoración, gestión y tratamiento de los riegos que pueden afectar su seguridad, con el propósito de implementar medidas y controles efectivos que les permitan estar preparados ante situaciones adversas que puedan comprometer tanto la seguridad física y lógica de sus instalaciones, personas, recursos y sistemas, como la seguridad de su información.

GLOSARIO

- Activo: En cuanto a la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

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

- Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- 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.

- Guía: documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas de información.

- Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. • Norma: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

- Parte interesada: (Stakeholder) Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

- Política del SGSI: Manifestación expresa de apoyo y compromiso de la alta dirección con respecto a la seguridad de la información.

- Política: Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la entidad.

- Procedimiento: Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.

- 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

- Sistema de Gestión de Seguridad de la Información SGSI o MSPI: 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, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

OBJETIVOS

OBJETIVO GENERAL

Establecer un documento de lineamientos de buenas prácticas en Seguridad y Privacidad para la Alcaldía de La Estrella.

OBJETIVOS ESPECIFICOS

- Mediante la utilización del Modelo de Seguridad y Privacidad para las Entidades del Estado, se busca contribuir al incremento de la transparencia en la gestión pública.
- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas en las entidades.
- Contribuir a mejorar los procesos de intercambio de información pública.
- Orientar a las entidades en las mejores prácticas en seguridad y privacidad.
- Optimizar la gestión de la seguridad de la información al interior de las entidades.
- Orientar a las entidades en la transición de lPv4 a IPv6 con la utilización de las guías disponibles para tal fin.
- Orientar a las entidades en la adopción de la legislación relacionada con la protección de datos personales.
- Contribuir en el desarrollo del plan estratégico institucional y la elaboración del plan estratégico de tecnologías de la información y de las comunicaciones. Contribuir en el desarrollo del ejercicio de arquitectura empresarial apoyando en el cumpliendo de los lineamientos del marco de referencia de arquitectura empresarial para la gestión de TI del estado colombiano.
- Orientar a las entidades destinatarias en las mejores prácticas para la construcción de una política de tratamiento de datos personales respetuosa de los derechos de los titulares.
- Optimizar la labor de acceso a la información pública al interior de las entidades destinatarias.
- Revisar los roles relacionados con la privacidad y seguridad de la información al interior de la entidad para optimizar su articulación.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

En el presente Modelo de Seguridad y Privacidad de la Información se contemplan 6 niveles de madurez, que corresponden a la evolución de la implementación del modelo de operación.

La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno en línea, permite alinearse al componente de TIC para la Gestión al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la

confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad.

La Seguridad y Privacidad de la Información se alinea al componente de TIC para Servicios apoyando el tratamiento de la información utilizada en los trámites y servicios que ofrece la Entidad, observando en todo momento las normas sobre protección de datos personales, así como otros derechos garantizados por la Ley que exceptúa el acceso público a determinada información.

El componente de TIC para Gobierno Abierto se alinea con el componente de Seguridad y Privacidad de la Información que permite la construcción de un estado más transparente, colaborativo y participativo al garantizar que la información que se provee tenga controles de seguridad y privacidad de tal forma que los ejercicios de interacción de información con el ciudadano, otras entidades y la empresa privada sean confiables.

DESCRIPCION DEL CICLO DE OPERACIÓN

En el presente capítulo se explica el ciclo de funcionamiento del modelo de operación, a través de la descripción detallada de cada una de las cinco (5) fases que lo comprenden. Estas, contienen objetivos, metas y herramientas (guías) que permiten que la seguridad y privacidad de la información sea un sistema de gestión sostenible dentro de las entidades.

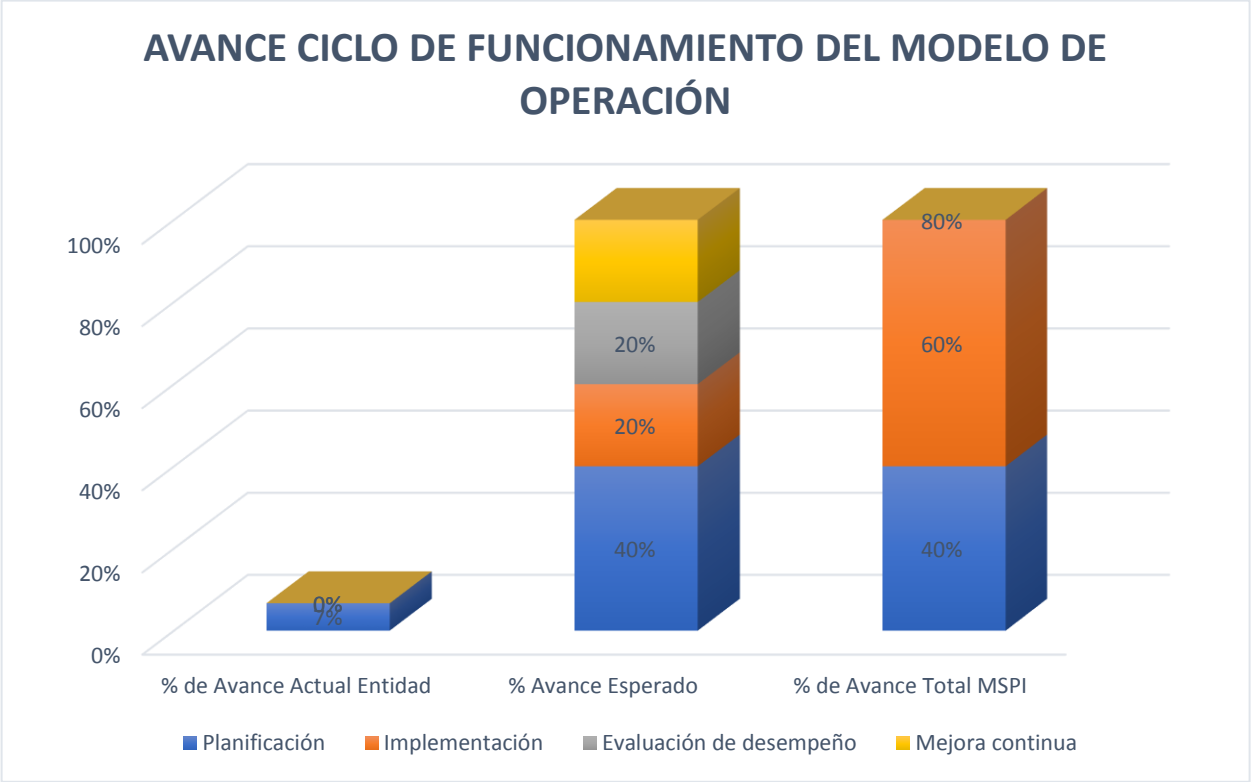
Figura 1 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

FASE DE DIAGNOSTICO – ETAPAS PREVIAS A LA IMPLEMENTACION

En esta fase se pretende identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información, para lo fue utilizada la herramienta de diagnóstico "articles-5482_Instrumento_Evaluacion_MSPI.xls", la cual nos permitió determinar lo siguiente:

Figura 2 – Etapas previas a la implementación

Estado actual de la gestión de seguridad y privacidad de la información al interior de la entidad



No.	Evaluación de Efectividad de controles			
	DOMINIO	**Calificación Actual**	**Calificación Objetivo**	**EVALUACIÓN DE EFECTIVIDAD DE CONTROL**
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	20	60	**INICIAL**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	4	60	**INICIAL**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	3	60	**INICIAL**
A.8	GESTIÓN DE ACTIVOS	14	60	**INICIAL**
A.9	CONTROL DE ACCESO	8	60	**INICIAL**
A.10	CRIPTOGRAFÍA	0	60	**INEXISTENTE**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	10	60	**INICIAL**
A.12	SEGURIDAD DE LAS OPERACIONES	6	60	**INICIAL**
A.13	SEGURIDAD DE LAS COMUNICACIONES	0	60	**INEXISTENTE**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	0	60	**INEXISTENTE**
A.15	RELACIONES CON LOS PROVEEDORES	0	60	**INEXISTENTE**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	60	**INEXISTENTE**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0	60	**INEXISTENTE**
A.18	CUMPLIMIENTO	5	60	**INICIAL**
PROMEDIO EVALUACIÓN DE CONTROLES		**5**	**60**	**INICIAL**

Nivel de madurez de los controles de seguridad de la información.

NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

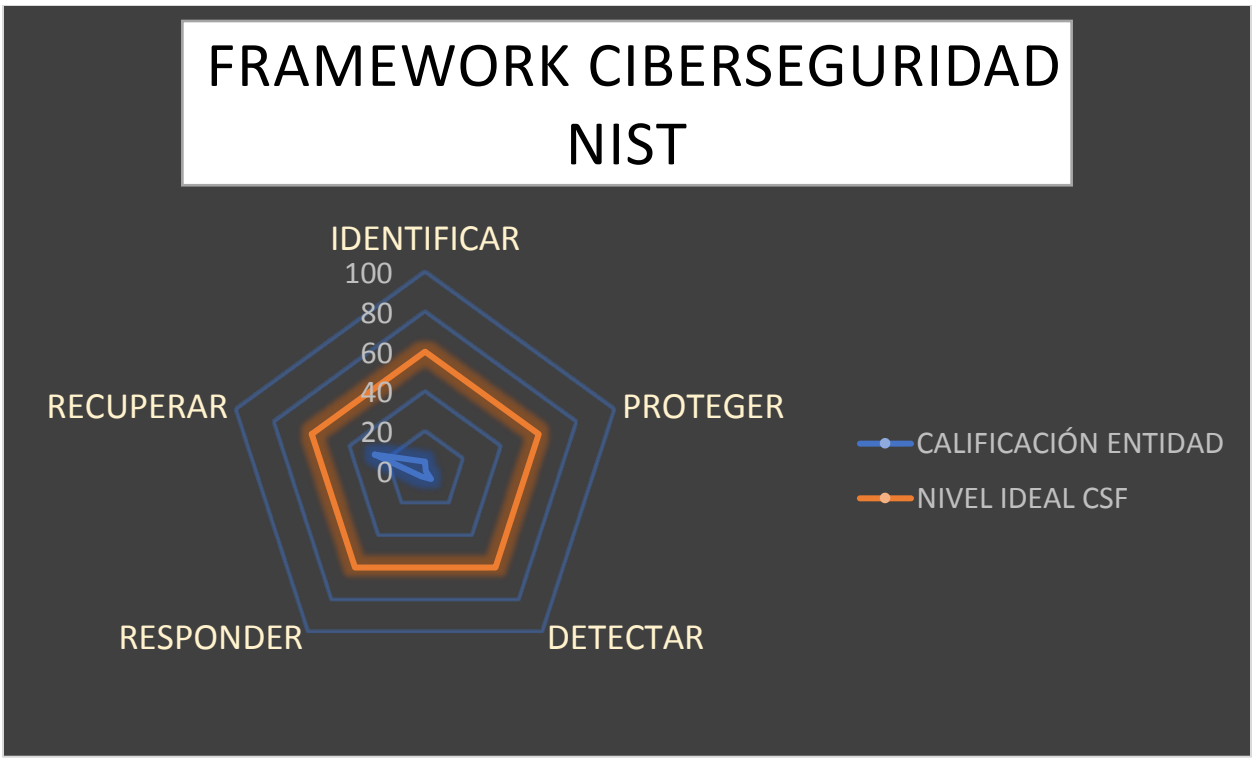
	NIVEL DE CUMPLIMIENTO
Inicial	INTERMEDIO
Gestionado	CRÍTICO
Definido	CRÍTICO
Gestionado Cuantitativamente	CRÍTICO
Optimizado	CRÍTICO

Nivel	Descripción
Inicial	En este nivel se encuentran las Entidades, que aún no cuentan con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información.
Gestionado	En este nivel se encuentran las Entidades, en las cuales existen procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentran gestionados dentro del componente de planificación del MSPI.
Definido	En este nivel se encuentran las Entidades que tiene documentado, estandarizado y aprobado por la dirección, el modelo seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Gestionado cuantitativamente	En este nivel se encuentran las Entidades, que cuenten con métricas, indicadores y realizan auditorías al modelo de seguridad y privacidad de la información, recolectando información para establecer la efectividad de los controles.
Optimizado	En este Nivel se encuentran las Entidades, en donde existe un mejoramiento continuo del modelo de seguridad y privacidad de la información, retroalimentación cualitativa del modelo.

Identificar el avance de la implementación del ciclo de operación al interior de la entidad.

Año	AVANCE PHVA			
	COMPONENTE	**% de Avance Actual Entidad**	**% Avance Esperado**	**% de Avance Total MSPI**
2015	Planificación	7%	40%	40%
2016	Implementación	0%	20%	60%
2017	Evaluación de desempeño	0%	20%	80%
2018	Mejora continua	0%	20%	100%
TOTAL				**7%**

Identificación del uso de buenas practicas en ciberseguridad.



Anexo: articles-5482_Instrumento_Evaluacion_MSPI.xls

Con el diagnostico obtenido, se determina que la entidad debe de trabajar arduamente en crear un MSPI ya que los resultados son bajos y estos indican el nivel alto de falta de estrategias que permitan la seguridad de la información. Manifestado lo anterior se definirá la ruta para avanzar en la gestión de seguridad y privacidad de la información al interior de la entidad, en la implementación de los controles de seguridad y privacidad de la información y apoyados en los establecidos en la ISO 27002, implementar buenas prácticas que permitan el ciclo de operación de operación al interior de la entidad, el nivel de cumplimiento de la normatividad vigente e identificación del buen uso en temas de ciberseguridad.

FASE DE PLANIFICACIÓN

Para el desarrollo de esta fase la Alcaldía de La Estrella utilizará los resultados de la etapa anterior y procederá a elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

- Política general de seguridad y privacidad de la información

La Política de Seguridad y Privacidad de la información está contenida en un documento de alto nivel que incluye la voluntad de la Alta Dirección de la Entidad para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información. La política debe contiene una declaración general por parte de la administración, donde se especifique sus objetivos, alcance, nivel de cumplimiento. La política debe ser aprobada y divulgada al interior de la entidad

Anexo: Política General de Seguridad de La Informacion.pdf

- Política de Seguridad y Privacidad de la Información

Manual de políticas, donde se describe los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los Activos de información al interior de la Entidad; definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información En el manual de políticas de la entidad, se debe explicar de manera general, las políticas, los principios de seguridad y la normatividad pertinente. La entidad debe evaluar los requerimientos necesarios para ser ajustados o desarrollados en la elaboración de las políticas de seguridad y privacidad, así como en la implementación.

Anexo: Políticas específicas de Seguridad de La Informacion.pdf

- Procedimientos de Seguridad de La Información

se debe desarrollar y formalizar procedimientos que permitan gestionar la seguridad de la información en cada uno de los procesos definidos en la entidad.

Actualmente la entidad cuenta con un Sistema de Gestión de Calidad, donde el área encargada tiene establecido 2 procedimientos, los cuales son los siguientes:

PR-SI-01 Procedimiento Mantenimiento Correctivo y Preventivo

PR-SI-02 Procedimiento Soporte Técnico

Anexo: Proceso Sistemas de información

Cabe mencionar que la entidad no cuenta con un visón que permita dimensionar la estructura y el debido funcionamiento tecnológico, ya que no cuentan con la infraestructura tecnológica adecuada y sus operaciones están encaminadas solamente el mantenimiento y reparación de lo que posee. No cuentan con una debida estructura tanto orgánica con en infraestructura TI.

- Responsabilidades y Roles de Seguridad y Privacidad de la Información

La entidad debe definir mediante un acto administrativo (Resolución, circular, decreto, entre otros) los roles y las responsabilidades de seguridad de la información en los

diferentes niveles (Directivo, De procesos y Operativos) que permitan la correcta toma de decisiones y una adecuada gestión que permita el cumplimiento de los objetivos de la Entidad.

Para desarrollar estas actividades, la Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información, brinda información relacionada para tal fin.

- Inventario de Activos de Información

La entidad debe desarrollar una metodología de gestión de activos que le permita generar un inventario de activos de información exacto, actualizado y consistente, que a su vez permita definir la criticidad de los activos de información, sus propietarios, custodios y usuarios.

Basados en la La Guía No 5 - Gestión De Activos, brinda información relacionada para poder llevar a cabo la realización de las actividades mencionadas previamente, por lo tanto, la entidad levanto el siguiente listado de activos de información “Registro de Activos de Informacion.xls”

Anexo: Registro de Activos de Informacion.xls

- Integración del MSP con el Sistema de Gestión Documental

La entidad deberá alinear la documentación relacionada con seguridad de la información con el sistema de gestión documental generado o emitido conforme a los parámetros emitidos por el archivo general de la nación.

La entidad con la construcción del PINAR, PGD y PGD, alineo estas directrices con el MSPI de la entidad.

- Anexo: PINAR-ARCHIVO
- POLITICA DE LA GESTION DOCUMENTAL

PROGRAMA DE GESTIÓN DOCUMENTAL MUNICIPIO DE LA ESTRELLA

- Identificación, Valoración y Tratamiento de Riesgos

La entidad debe definir una metodología de gestión del riesgo enfocada a procesos, que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos, así como la declaración de aplicabilidad. Para conseguir una integración adecuada entre el MSPI y la guía de gestión del riesgo emitida por el DAFP respecto a este procedimiento, se recomienda emplear los criterios de evaluación (impacto y probabilidad) y niveles de riesgo emitidos por esta entidad.

Para definir la metodología, la entidad puede hacer uso de buenas prácticas vigentes tales como: ISO 27005, Margerit, Octave, ISO 31000 o la Guía No 7 - Gestión de Riesgos

emitida por el MinTIC. Para la elaboración del plan de tratamiento de riesgos y la declaración de aplicabilidad, puede emplearse la Guía No 8 - Controles de Seguridad.

La entidad identifico, valoro y lleva el tratamiento de los riesgos, los cuales se manifiestan en el documento de Excel Riesgos de información.xls

Anexo: Riesgos de información.xls

- Plan de Comunicaciones

La Entidad debe definir un Plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, terceros) de la entidad.

Este plan será ejecutado, con el aval de la Alta Dirección, a todas las áreas de la Entidad.

Para estructurar dicho plan puede utilizar la Guía No 14 – plan de comunicación, sensibilización y capacitación.

- Plan de transición de IPv4 a IPv6

Para llevar a cabo el proceso de transición de IPv4 a IPv6 en las entidades, se debe cumplir con la fase de planeación establecida en la Guía No 20 - Transición de IPv4 a IPv6 para Colombia que indica las actividades específicas a desarrollar.

Indicadores

RELACIONADOS EN MARCO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
DEFINICIÓN		
El indicador permite determinar la eficiencia en el tratamiento de eventos relacionados la seguridad de la información. Los eventos serán reportados por los usuarios o determinadas en las auditorías planeadas para el sistema.		
OBJETIVO		
El objetivo del indicador es reflejar la gestión y evolución del modelo de seguridad y privacidad de la información al interior de una entidad		
TIPO DE INDICADOR		
Indicador de Gestión		
DESCRIPCIÓN DE VARIABLES	**FORMULA**	**FUENTE DE INFORMACIÓN**
VSI05: Número de anomalías cerradas.	(VSI05/VSI06)*100	Auditorías internas, herramientas de monitoreo
VSI06: Número total de anomalías encontradas.		Auditorías internas, herramientas de monitoreo
METAS		

MÍNIMA	75-80%	**SATISFACTORIA**	80- 90%	**SOBRESALIENTE**	100%

PLAN DE COMUNICACIONES					
DEFINICIÓN					
El indicador permite medir la aplicación de los temas sensibilizados en seguridad de la información por parte de los usuarios finales. Estas mediciones se podrán realizar por medio de auditorías especializadas en el tema o de forma aislada por parte de los responsables de la capacitación y sensibilización.					
OBJETIVO					
El objetivo del indicador es establecer la efectividad de un plan de capacitación y sensibilización previamente definido como medio para el control de incidentes de seguridad.					
TIPO INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES		**FORMULA**		**FUENTE DE INFORMACIÓN**	
VSI07: Número de fallas o no cumplimientos encontrados en las sensibilizaciones programadas o eventos realizados para evaluar el tema.		(VSI07/VSI08)*100		Oficial de Seguridad de la Información, auditorías internas, atención al usuario, listas de asistencia	
VSI08: Total de personal a capacitar.			Total de funcionarios de la entidad.		
METAS					
MÍNIMA	75-80%	**SATISFACTORIA**	80- 90%	**SOBRESALIENTE**	100%
OBSERVACIONES					
Para el levantamiento de la información que permita obtener datos para la medición el responsable debe idear planes, laboratorios o actividades periódicas que permitan medir lo capacitado o divulgado.					

DECRETO N°

(25 OCT 2019) 172

POR MEDIO DEL CUAL SE ADOPTA EL MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACION, MANUAL DE POLITICA PARA EL TRATAMIENTO DE DATOS PERSONALES Y POLITICA DE SEGURIDAD DE LA INFORMACION DEL SITIO WEB

El Alcalde del Municipio de La Estrella - Antioquia, en uso de sus facultades constitucionales y legales, en especial las conferidas por los Artículos 315 de la Constitución Política, 91 de la Ley 136 de 1994, la Ley 594 de 2000, Ley 1266 de 2008, Ley 1551 de 2012, Ley 1581 2012, Ley 1712 de 2014, Decreto 1083 de 2015 modificado y adicionado por el Decreto 648 de 2017, Decreto 1499 de 2017, Decreto 1008 de 2018, y

CONSIDERANDO:

1. Que las políticas de seguridad de la información y protección de datos personales tienen por objeto establecer los lineamientos de índole técnico y organizacional necesarios para garantizar la seguridad y el uso adecuado de los sistemas informáticos y la información de La Alcaldía de La Estrella, por parte de todos los funcionarios públicos y personal que haga uso de ellos.

2. Que la información es uno de los activos más importante de la Entidad, por lo tanto, debe estar protegida implementando parámetros mínimos para su administración, protección y utilización adecuada, toda vez que dichas políticas serán la base de la seguridad de la información de la Entidad.

3. Que para La Alcaldía del Municipio de La Estrella es una prioridad preservar la confidencialidad, integridad y disponibilidad de la información, por lo tanto, es deber de todos los servidores públicos y/o usuarios de la entidad, proteger y hacer una adecuada utilización de los recursos tecnológicos disponibles.

4. Que la Ley 1581 de 2012, "*Por la cual se dictan disposiciones generales para la protección de datos personales*" reglamentado por el Decreto 1377 de 2013, incorporo los lineamientos necesarios para que las entidades públicas y privadas identificaran los roles y la tipología de datos que son objeto de protección constitucional, así mismo, dispuso las condiciones para las cuales se deben recolectar los datos personales y que posteriormente serán vinculados con la administración de una base de datos.

5. Que la Ley 1712 de 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"*, estableció los procedimientos para el ejercicio y garantías del registro de activos de información;

6. Que el Decreto 1499 de 2017, *"Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015"*, en lo relacionado con el Sistema de Gestión MIPG; en su artículo 2.2.22.2.1. (Políticas de Gestión y Desempeño Institucional) estable que "*Las políticas de Desarrollo Administrativo de que trata la Ley 489 de 1998, formuladas por el Departamento Administrativo de la Función Pública y los demás líderes, se denominarán políticas de Gestión y Desempeño Institucional y comprenderán, entre otras, las siguientes:. Numeral 12: Seguridad digital….*

7. Que el Decreto 1008 de 2018, *"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones*", Artículo 2.2.9.1.2.1 (estructura de los elementos de la Política de Gobierno Digital) establece que "*La Política de Gobierno Digital será definida por el Ministerio de Tecnologías de Información y las Comunicaciones y se desarrollará a través de componentes y habilitadores transversales que, acompañados de lineamientos y estándares, permitirán el logro de propósitos que generarán valor público en un entorno de confianza digital a partir del aprovechamiento de las TIC"*....

8. Que mediante el Decreto 024 de febrero 27 de 2019, se creó el Comité Municipal de Gestión y Desempeño del Municipio de La Estrella, siendo este un órgano asesor, articulador e impulsor de iniciativas para la correcta implementación, operación, desarrollo, evaluación y seguimiento del Modelo Integrado de Planeación y Gestión – MIPG a nivel Municipal; y según el artículo tercero define por quienes está integrado, y en el numeral 1° de dicho artículo se establece que el Alcalde Municipal será quien preside dicho comité.

9. Que el Artículo Cuarto, numeral 5 del Decreto 024 de febrero 27 de 2019, reza lo siguiente:" Dirigir *y articular a las entidades del municipio en la implementación y operación de las políticas de gestión y desempeño y de las directrices impartidas por la Presidencia de la Republica y el Ministerio de tecnologías de información y las Comunicaciones en materia de Gobierno y seguridad Digital"*..

10. Que por medio del CONPES 3701 de 2011 se fijaron los lineamientos de la política para la Ciberseguridad y Ciberdefensa.

11. Que por medio del CONPES 3854 de 2016 se fijó la política Nacional de seguridad digital, para que las entidades del Estado constituyan mecanismos para la gestión de los riesgos digitales.

12. Que el día quince (15) de agosto de 2019, se reunió el Comité Municipal de Gestión y Desempeño del Municipio de La Estrella con el fin de revisar y aprobar el Manual de Políticas de Seguridad de la Información, manual de Política para el Tratamiento de Datos Personales y Política de Seguridad de la Información del Sitio web de la Alcaldía de La estrella, así como de políticas específicas recomendadas para la implementación.

13. Que producto de la reunión mencionada en el punto anterior, se levantó el acta N° 001 mediante la cual surgieron los siguientes compromisos: A) Revisar los tres documentos para su aprobación. B) Aprobación del Manual Política de Tratamiento de Datos Personales, Plan Estratégico de tecnologías de la Información PETI y Políticas específicas recomendadas para la implementación.

14. Que una vez cumplidos los compromisos adquiridos en el acta N° 001 de 2019 de: A) Revisar los tres documentos para su aprobación. B) Aprobación del Manual Política de Tratamiento de Datos Personales, Plan Estratégico de tecnologías de la Información PETI y Políticas específicas recomendadas para la implementación; el Comité Municipal de Gestión y Desempeño del Municipio de La Estrella aprobó la adopción del manual de políticas de seguridad de la información, manual de política para el tratamiento de datos personales y política de seguridad de la información del sitio web.

Que, en mérito de lo expuesto, el alcalde del Municipio de La Estrella;

DECRETA:

ARTÍCULO PRIMERO: Adoptar, el manual de Políticas de Seguridad de la Información, manual de Política para el Tratamiento de Datos Personales y Política de Seguridad de la Información del Sitio web de la Alcaldía de La Estrella, Antioquia.

ARTÍCULO SEGUNDO: Campo de aplicación, las disposiciones del presente Decreto se aplicarán a todo el personal que labore en, o, para La Alcaldía de La Estrella, con el fin de garantizar el cumplimiento en los requerimientos de confidencialidad, integridad y disponibilidad de la información.

Todos los servidores públicos/contratistas y/o terceros que utilicen los recursos tecnológicos de la Entidad, tienen la responsabilidad de protegerlos y hacer buen uso de estos.

ARTÍCULO TERCERO: Regular las políticas, alcance, objetivos y procedimientos relacionados con la seguridad y privacidad de la información, protección de datos personales, conforme a lo señalado en el presente Decreto.

ARTÍCULO CUARTO: Las disposiciones del presente Decreto aplican a los procesos estratégicos, misionales, de apoyo y de evaluación de la Alcaldía de La Estrella.

172

ARTÍCULO QUINTO: La implementación de los manuales de Política de Seguridad de la Información, Política de Tratamiento de Datos Personales y Política de seguridad de La Información del Sitio web, deberán ser conocidas y cumplidas por todos los funcionarios, contratistas, proveedores, ciudadanía en general y demás partes interesadas, que accedan a los recursos tecnológicos de la Entidad.

ARTICULO SEXTO: Publíquense, manual de Políticas de Seguridad de la Información, manual de Política para el Tratamiento de Datos Personales y Política de Seguridad de la Información del Sitio web de la Alcaldía de La estrella - Antioquia, en la página web e intranet de la Entidad.

ARTÍCULO SEPTIMO: El presente Decreto rige a partir de su expedición.

Dado en el Municipio de La Estrella (Antioquia), a los 25 OCT 2019

PUBLIQUESE, COMUNIQUESE Y CÚMPLASE

JHONNY ALEXANDER GARCIA YEPES
Alcalde

Proyectó: German López	FIRMA
Revisión Jca: Ramón Morales Rueda	FIRMA

100.14

MANUAL POLITICAS ESPECÍFICAS SEGURIDAD DE LA INFORMACION

CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se agruparán las políticas con el objetivo de hacer una implementación transversal de Seguridad de la Información en la Entidad.

1.1. POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Dando cumplimiento a las actividades desarrolladas en la implementación del Modelo de Seguridad y Privacidad de la Información que se encuentra realizando LA ALCALDIA DE LA ESTRELLA, se elaboran una serie de políticas que se describen a continuación:

1.1.1. *POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN*

La Alcaldía de La Estrella se compromete a otorgar los recursos necesarios para garantizar los tres (3) pilares fundamentales de la Seguridad como son la disponibilidad, integridad y confidencialidad de la información, con el fin de dar cumplimiento a los objetivos institucionales, la estrategia y misión de La Alcaldía de La Estrella.

La Alta Dirección de la entidad se compromete a velar por la aplicación y cumplimiento adecuado de la presente política de seguridad de la información y todas las que se deriven de ella, por parte de todos los funcionarios de la Entidad, terceros, aprendices, practicantes, proveedores y la ciudadanía en general del Municipio de La Estrella.

La Alcaldía de La Estrella se compromete a cumplir con todos los requisitos legales, reglamentarios y contractuales a que haya a lugar, con el fin de gestionar y reducir los riesgos a un nivel aceptable.

Establecer la mejora continua para la Seguridad de la Información, a través de un conjunto de reglas y directrices orientadas a garantizar la protección de los activos de información de La Alcaldía de La Estrella, de una manera contundente, eficiente y efectiva, y de la misma forma velar por tomar las acciones necesarias para la evaluación, análisis y tratamiento de los riesgos de acuerdo con la metodología adoptada por La Alcaldía de La Estrella.

1.1.2. *POLÍTICA DE PRIVACIDAD*

La Alcaldía de La Estrella, se compromete a otorgar los recursos necesarios para garantizar los tres (3) pilares fundamentales de la privacidad de la información como son la finalidad, confidencialidad, integridad y disponibilidad de la información.

La Dirección General se compromete a velar por la aplicación y cumplimiento adecuado de la presente política de privacidad de la información y todas las que se deriven de ella, por parte de todos los funcionarios, Colaboradores y Terceros de LA ALCALDIA DE LA ESTRELLA.

La Alcaldía de La Estrella reconoce que el único medio autorizado para el tratamiento de datos personales es el titular de la información, de acuerdo con la Ley de protección de datos personales 1581 de 2012 decreto 1377 de 2013 o la que la adicione, modifique o derogue.

1.1.3. *POLÍTICA DE ROLES Y RESPONSABILIDADES*

Objetivo: Definir los Roles y Responsabilidades en Seguridad de la Información en La Alcaldía de La Estrella.

Todos los funcionarios, Colaboradores y Terceros que ejercen funciones en La Alcaldía de La Estrella y previamente han sido autorizados para acceder a los recursos tecnológicos y de procesamiento de información de La Alcaldía de La Estrella, son responsables del cumplimiento de las políticas, procedimientos y normatividad vigente definida por La Alcaldía.

Responsabilidades Alta Dirección - Oficina de tecnologías de la información y/o sistemas de la entidad:

- Establecer, mantener y divulgar las políticas y procedimientos de servicios de tecnología, incluida esta política de seguridad de información y todos sus capítulos, el uso de los servicios tecnológicos en toda la entidad de acuerdo con las mejores prácticas y lineamientos de la Alta Dirección y directrices del Gobierno.
- Mantener la custodia de la información que reposa en los diferentes sistemas de información, bases de datos y aplicativos de la Institución.
- Informar de los eventos que estén en contra de la seguridad de la información y de la infraestructura tecnológica de la Institución a la Alta Dirección, las diferentes secretarias de despacho de La ALCALDIA DE LA

ESTRELLA, así como a los entes de control e investigación que tienen injerencia sobre la entidad.

- Proporcionar medidas de seguridad físicas, lógicas y procedimentales para la protección de la información digital de la Entidad.
- Aplicar y hacer cumplir la Política de Seguridad de la Información y sus componentes.
- Administrar las reglas y atributos de acceso a los equipos de cómputo, sistemas de información, aplicativos y demás fuentes de información al servicio LA ALCALDIA DE LA ESTRELLA.
- Analizar, aplicar y mantener los controles de seguridad implementados para asegurar los datos e información gestionados en la Institución.
- Resolver de común acuerdo con las áreas y los propietarios de la información los conflictos que se presenten por la propiedad de la información al interior de la entidad. Esto incluye los posibles medios de acceso a la información, los datos derivados del procesamiento de la información a través de cualquier aplicación o sistema, los datos de entrada a las aplicaciones y los datos que son parte integral del apoyo de la solicitud.
- Habilitar/Deshabilitar el reconocimiento y operación de Dispositivos de Almacenamiento externo de acuerdo con las directrices emitidas de parte de la Dirección General y las diferentes direcciones.
- Implementar los mecanismos de controles necesarios y pertinentes para verificar el cumplimiento de la presente política.

Responsabilidades grupo de soporte técnico de la entidad.

- Garantizar la disponibilidad de los servicios y así mismo programar o informar a todos los usuarios cualquier problema o mantenimiento que pueda afectar la normal prestación de los mismos; así como gestionar su acceso de acuerdo con las solicitudes recibidas de las diferentes Direcciones, Jefaturas o Coordinaciones siguiendo el procedimiento establecido.
- Establecer, mantener y divulgar las políticas y procedimientos de los servicios de tecnología, incluidos todos los capítulos que hacen parte de esta Política, de acuerdo con las mejores prácticas y directrices de la Entidad y del Gobierno.
- Determinar las estrategias para el mejoramiento continuo del servicio tecnológico, la optimización de los recursos tecnológicos, las mejoras en los sistemas de información con miras a un gobierno de tecnologías consolidado.

- Brindar el soporte necesario a los usuarios a través de los canales de mesa de ayuda actualmente implementados en la institución.

Responsabilidades de los propietarios de la información

- Son propietarios de la información cada uno de los Secretarios de Despacho, Subsecretarios de Despacho de las oficinas donde se genera, procesa y mantiene información, en cualquier medio, propia del desarrollo de sus actividades.
- Valorar y clasificar la información que está bajo su administración y/o generación.
- Autorizar, restringir y delimitar a los demás usuarios de la institución el acceso a la información de acuerdo con los roles y responsabilidades de los diferentes funcionarios, contratistas o practicantes que por sus actividades requieran acceder a consultar, crear o modificar parte o la totalidad de la información.
- Determinar los tiempos de retención de la información en conjunto con él grupo de Gestión Documental y Correspondencia y las áreas que se encarguen de su protección y almacenamiento de acuerdo con las determinaciones y políticas de la entidad como de los entes externos y las normas o leyes vigentes.
- Determinar y evaluar de forma permanente los riesgos asociados a la información, así como los controles implementados para el acceso y gestión de la administración comunicando cualquier anomalía o mejora tanto a los usuarios como a los custodios de esta.
- Acoger e informar los requisitos de esta política a todos los funcionarios, contratistas y practicantes en las diferentes dependencias del Instituto.

Responsabilidades de los funcionarios, contratistas y practicantes usuarios de la información

- Utilizar solamente la información necesaria para llevar a cabo las funciones que le fueron asignadas, de acuerdo con los permisos establecidos o aprobados en el Manual de Funciones, Código Disciplinario Único – Ley 734 de 2002 y/o Contrato.
- Manejar la Información de la Entidad y rendir cuentas por el uso y protección de dicha información mientras que este bajo su custodia. Esta puede ser física o electrónica e igualmente almacenada en cualquier medio.
- Proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
- Evitar la divulgación no autorizada o el uso indebido de la información.

- Cumplir con todos los controles establecidos por los propietarios de la información y los custodios de esta.
- Informar a sus superiores sobre la violación de estas políticas o si conocen de alguna falta a alguna de ellas.
- Proteger los datos almacenados en los equipos de cómputo y sistemas de información a su disposición de la destrucción o alteración intencional o no justificada y de la divulgación no autorizada.
- Reportar los Incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.
- Proteger los equipos de cómputo, comunicaciones y demás dispositivos tecnológicos o técnico/científico designados para el desarrollo de sus funciones. No está permitida la conexión de equipos de cómputo y de comunicaciones ajenos a la red Institucional de la Entidad, ni el uso de dispositivos de acceso externo a Internet o de difusión de señales de red que no hayan sido previamente autorizadas por la Oficina de Sistemas de la entidad.
- Usar software autorizado que haya sido adquirido legalmente por la Entidad. No está permitido la instalación ni uso de software diferente al Institucional sin el consentimiento de sus superiores y visto bueno de la Oficina de Sistemas.
- Divulgar, aplicar y el cumplir con la presente Política de seguridad de La información.
- Aceptar y reconocer que en cualquier momento y sin previo aviso, la oficina de control interno y/o jefe de despacho encargado puede solicitar una inspección de la información a su cargo sin importar su ubicación o medio de almacenamiento. Esto incluye todos los datos y archivos de los correos electrónicos institucionales, sitios web institucionales y redes sociales propiedad de la Entidad, al igual que las unidades de red institucionales, computadoras, servidores u otros medios de almacenamiento propios de la Entidad. Esta revisión puede ser requerida para asegurar el cumplimiento de las políticas internamente definidas, por actividades de auditoría y control interno o en el caso de requerimientos de entes fiscalizadores y de vigilancia externos, legales o gubernamentales.
- Proteger y resguardar la información personal que no esté relacionada con sus funciones en la Entidad. El Municipio no es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas débito/crédito.
-

1.1.4. *POLÍTICA DE DISPOSITIVOS MÓVILES*

Objetivo: Proteger la información almacenada en dispositivos móviles de La Alcaldía de La Estrella. Se debe llevar un registro y control de todos los dispositivos móviles que posee la entidad.

Todos los funcionarios, terceros, aprendices, practicantes, proveedores y ciudadanía en general deben hacer buen uso de los dispositivos móviles que son asignados para el desempeño de sus funciones laborales.

Los dispositivos móviles que estén autorizados para salir y que contengan información sensible, se deben proteger mediante el uso de controles tecnológicos apropiados para ello, como cifrado de información, políticas de Restricción en la ejecución de aplicaciones, y de conexión de dispositivos USB, inactivación de accesos inalámbricos cuando se encuentren conectadas a la red LAN, entre otros.

Todos los dispositivos móviles que almacenen información de La Alcaldía del municipio de La Estrella deben contar con un sistema de autenticación, como un patrón de movimiento, un código de desbloqueo o una clave.

Todos los dispositivos móviles que almacene información de La Alcaldía de La Estrella deben tener instalado un software de antivirus.

Todos los dispositivos móviles que son propiedad de La Alcaldía de La Estrella pueden estar monitoreados y ser sometidos a la aplicación de controles en cuanto a tipo, versión de aplicaciones instaladas, contenido restringido y de ser necesario se podrá restringir conexiones hacia ciertos servicios de información que sean considerados maliciosos.

Los funcionarios, terceros, aprendices, practicantes, proveedores, responsable del dispositivo móvil debe hacer periódicamente copias de respaldo, en caso de los portátiles deben conectar el equipo mínimo una vez por semana a la red, con el fin de que se ejecute la copia de respaldo de la carpeta destinada para esta función.
Todos los funcionarios, terceros, aprendices, practicantes, proveedores son responsables de garantizar el buen uso de los dispositivos móviles en redes seguras y con la protección adecuada para evitar acceso o divulgación no autorizada de la información almacenada y procesada en ellos.

Todos los dispositivos móviles propiedad de los funcionarios, terceros, aprendices, practicantes, proveedores, que requieran tener acceso a los componentes tecnológicos como el correo electrónico de La Alcaldía de La Estrella, deben solicitar autorización mediante el procedimiento formal de autorización de ingreso a la red y estar debidamente identificados, con el fin de llevar el control y garantizar que se implementen las medidas de aseguramiento necesaria

definidas por la Oficina de Sistemas, de esta forma se puede garantizar la preservación de la disponibilidad, confidencialidad e integridad de la información de La Alcaldía de La Estrella.

1.1.5. *SEGURIDAD DE LOS RECURSOS HUMANOS*

Objetivo: Garantizar la protección de la disponibilidad, integridad y confidencialidad de la información del personal que trabaja para La Alcaldía de La Estrella, a través de mecanismos de validación y concientización del recurso humano que hará uso de esta.

Incorporación de la Seguridad en la matriz de Cargos de La Alcaldía de La Estrella

Deben ser incorporadas los roles y responsabilidades en seguridad de la información, en la matriz de responsabilidades de La Alcaldía de La Estrella.

Control y Política del personal

Se deben definir controles de verificación del personal en el momento en que se postula al cargo. Estos controles incluirán todos los aspectos legales y de procedimiento que dicta el proceso de contratación de La Alcaldía de La Estrella.

Acuerdo de Confidencialidad

Todos los funcionarios, terceros, aprendices, practicantes, proveedores que ingresen a trabajar en La Alcaldía de La Estrella, deben firmar como parte de sus términos y condiciones iniciales de trabajo, un Acuerdo de Confidencialidad o no divulgación, en caso de que no estuviere incluido como una cláusula dentro del contrato de prestación de servicios o en el Acta de Posesión del funcionario. Este acuerdo debe incluir la aceptación de las políticas y lineamientos en Seguridad y Privacidad de la Información, el tratamiento de la información de La Alcaldía de La Estrella, en los términos de la Ley 1581 de 2012 y las demás normas que la adicionen, modifiquen, reglamenten o complementen, así como el Decreto 1377 de 2013 que reglamento la mencionada ley. Este documento debe ser archivado de forma segura por el área de Talento Humano y Contractual, según sea el caso.

Dentro del mismo acuerdo los funcionarios, terceros, aprendices, practicantes, proveedores declaran conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad ni los derechos de los funcionarios, terceros, aprendices, practicantes, proveedores.

Selección de personal

Dentro de los procesos de contratación de personal o de prestación de servicios, debe realizarse la verificación de antecedentes, de acuerdo con la reglamentación.

Se deben aplicar los controles establecidos por La Alcaldía de La Estrella para otorgar el acceso a la información CONFIDENCIAL o RESERVADA por parte del personal que resulte vinculado a La Alcaldía de La Estrella.

El área de Recursos humanos y Jurídica son los responsables de realizar la verificación de antecedentes disciplinarios, fiscales y judiciales y que se anexe la documentación requerida para la contratación.

Términos y condiciones Laborales

Todos los funcionarios, terceros, aprendices, practicantes, proveedores de La Alcaldía de La Estrella deben dar cumplimiento a las políticas y normatividad establecida en seguridad y privacidad de la información y debe ser parte integral de los contratos o documentos de vinculación a que haya lugar.

Todos los funcionarios, terceros, aprendices, practicantes, proveedores, durante el proceso de vinculación a La Alcaldía de La Estrella, deberán recibir una inducción sobre las Políticas y Lineamientos de Seguridad y Privacidad de la Información.

Entrenamiento, concientización y capacitación

Todos los funcionarios, terceros, aprendices, practicantes, proveedores de La Alcaldía de La Estrella deben ser entrenados y capacitados para las funciones, actividades y cargos que van a desempeñar, esto con el fin de sensibilizar a los usuarios sobre la protección adecuada de los recursos y la información de La Alcaldía de La Estrella. Así mismo, se debe garantizar la comprensión del alcance y contenido de las políticas y lineamientos de Seguridad de la información y la necesidad de respaldarlas y aplicarlas de manera permanente e integral desde su función.

Formación y Capacitación en Materia de Seguridad de la Información

Todos los funcionarios, terceros, aprendices, practicantes, proveedores cuando sea el caso, que trabajan para La Alcaldía de La Estrella deben recibir una adecuada capacitación y actualización periódica en materia de las políticas, normas y procedimientos de Seguridad y privacidad de la Información. dentro del contenido se deben contemplar los requerimientos de seguridad y las responsabilidades legales, así como la capacitación sobre el uso adecuado de

las instalaciones de procesamientos de información y los recursos tecnológicos informáticos que les provee La Alcaldía de La Estrella para el desempeño de sus funciones laborales y contractuales.

Procesos disciplinarios

Todos los incidentes de seguridad de la información presentados en La Alcaldía de La Estrella deben tener el tratamiento adecuado y establecido en el procedimiento de atención de incidentes de seguridad de la información, con el fin de determinar sus causas y responsables.

Del resultado de los procesos derivados de los reportes y del análisis de los Incidentes de seguridad y teniendo en cuenta el impacto y las responsabilidades identificadas, se tomarán acciones y se realizará el respectivo traslado ante las instancias correspondientes.

En lo pertinente a la violación de las políticas de seguridad de la información de La Alcaldía de La Estrella, a los funcionarios, terceros, aprendices, practicantes, proveedores, se les aplicará lo establecido en la ley, particularmente en el Código Único Disciplinario (Ley 734 de 2002), el Estatuto Anticorrupción (Ley 1474 de 2011) y demás normas que las adicionen, modifiquen, reglamenten o complementen.

1.1.6. *POLÍTICA DE USO DE CORREO ELECTRÓNICO*

Objetivo: definir las directrices generales del buen uso del correo electrónico institucional en La Alcaldía de La Estrella.

Usos aceptables del servicio

Se debe utilizar exclusivamente para las actividades propias del desempeño de las funciones o actividades laborales a desempeñar en La Alcaldía de La Estrella y no se debe utilizar para otros fines.

Se debe utilizar de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos o sistemas de información e imagen de La Alcaldía de La Estrella.

Todos los funcionarios, terceros, aprendices, practicantes, proveedores que son autorizados para acceder a la red de datos y los componentes de Tecnologías de Información son responsables de todas las actividades que se ejecuten con sus credenciales de acceso a los buzones de correo.

Todos los funcionarios, terceros, aprendices, practicantes, proveedores deben dar cumplimiento a la reglamentación y leyes, en especial la Ley 1273 de 2009 de Delitos Informáticos, así mismo evitar prácticas o usos que puedan comprometer la seguridad de la información de entidad.

El servicio de correo electrónico debe ser empleado para servir a una finalidad operativa y administrativa en relación con La Alcaldía de La Estrella.

Todas las comunicaciones establecidas mediante este servicio, sus buzones y copias de seguridad se consideran de propiedad de La Alcaldía de La Estrella y pueden ser revisadas por el administrador del servicio o cualquier instancia de vigilancia y control, en caso de una investigación o incidentes de seguridad de la información.

Cuando un proceso, oficina, grupo o dependencia, tenga información de interés institucional para divulgar, lo debe hacer a través de la Oficina de Comunicaciones de La Alcaldía de La Estrella o con la debida autorización de la oficina mencionada, también mediante el medio formal autorizado para realizar esta actividad.

Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por La Alcaldía de La Estrella y deberán conservar en todos los casos el mensaje legal corporativo. El único servicio de correo electrónico controlado en La Alcaldía de La Estrella es el asignado directamente por la Oficina de Sistemas, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para evitar ataques informáticos, virus, spyware y otro tipo de software o código malicioso.

Los demás servicios de correo electrónico son utilizados bajo responsabilidad directa y riesgo de los usuarios, siendo necesaria la aprobación y firma por parte del director, jefe de oficina, coordinador de rupo de trabajo o supervisor de contrato; de un documento de análisis de riesgos para la autorización de sistemas de correo electrónico diferentes al institucional.

Es responsabilidad del usuario etiquetar el mensaje de correo electrónico de acuerdo con los niveles de clasificación para los cuales se requiere etiquetado (Reservado o Confidencial), de acuerdo con la Clasificación y Etiquetado de la Información establecida en La Alcaldía de La Estrella.

El tamaño del buzón de correo electrónico se asigna de manera estandarizada, la capacidad específica es definida y administrada por la Oficina de Sistemas de La Alcaldía de La Estrella.

Todos los funcionarios, terceros, aprendices, practicantes, proveedores son responsables de informar si tienen accesos a contenidos o servicios que no estén autorizados y no correspondan a sus funciones o actividades designadas dentro de La Alcaldía de La Estrella, para que de esta forma la Oficina de Sistemas realicen el ajuste de permisos requerido.

El usuario debe reportar cuando reciba correos de tipo SPAM, es decir correo no deseado o no solicitado, correos de dudosa procedencia o con virus a la Oficina de Sistemas, con el fin de tomar las acciones necesarias que impidan el ingreso de ese tipo de correos. De la misma forma el usuario debe reportar cuando no reciba correos y este seguro que este no es de tipo SPAM, así la Oficina de Sistemas hacen el análisis para evaluar el origen y así tomar las medidas pertinentes.

Cuando un usuario se retire de La Alcaldía de La Estrella, y se le haya autorizado el uso de una cuenta con acceso a la red y a diferentes servicios, debe abstenerse de continuar empleándolas y debe verificar que su cuenta y acceso a los servicios sean cancelados, las secretarias de Despacho a través de sus funcionarios deben reportar a la oficina de sistemas al siguiente correo electrónico sistemas@laestrella.gov.co, para proceder a bloquear los accesos a la información y/o servicios tecnológicos a los que tenga acceso

Los mensajes y la información contenida en los buzones de correo son de propiedad de La Alcaldía de La Estrella.

Cada usuario se debe asegurar que, en el reenvío de correos electrónicos, la dirección de destino es correcta, de manera que esté siendo enviado a los destinatarios que son. Si tiene listas de distribución también se deben depurar. El envío de información a personas no autorizadas es responsabilidad de quien envía el mensaje de correo electrónico.

La información almacenada en los archivos de tipo PST es responsabilidad de cada uno de los usuarios y cada usuario debe realizar la depuración periódica del buzón para evitar que alcance su límite.

Todo usuario es responsable de reportar los mensajes cuyo origen sean desconocidos, y asume la responsabilidad de las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En los casos en que el funcionario, terceros, aprendices, practicantes, proveedores desconfíe del remitente de un correo electrónico debe remitir la consulta a la mesa de soporte técnico.

Si una cuenta de correo es interceptada por personas mal intencionadas o delincuentes informáticos o se reciba cantidad excesiva de correos no deseado (SPAM), la Oficina de Sistemas actuará según sea el caso.

La Oficina de Sistemas se reserva el derecho de filtrar los tipos de archivo que vengan con archivos adjuntos en formatos anexos al correo electrónico para evitar amenazas de virus y otros programas destructivos. Todos los mensajes electrónicos serán revisados para evitar que tengan virus u otro programa destructivo. Si el virus u otro programa destructivo no pueden ser eliminados, el mensaje será borrado.

Ningún funcionario, colaborador o tercero debe suscribirse en boletines en líneas, publicidad o que no tenga que ver con sus actividades laborales, con el correo institucional.

El funcionario, colaborar o tercero no debe responder mensajes donde les solicitan información personal o financiera que indican que son sorteos, ofertas laborales, ofertas comerciales o peticiones de ayuda humanitaria. Por el contrario, debe notificar a la Oficina de Sistemas, con el fin de ejecutar las actividades pertinentes como bloquear por remitente y evitar que esos mensajes lleguen a más buzones de correo de La Alcaldía de La Estrella.

Toda cuenta de correo @laestrella.gov.co es de propiedad de La Alcaldía de La Estrella y los buzones que no sean utilizados en un tiempo superior a cuarenta y cinco (45) días se inactivan por el responsable de correo electrónico.

Todo mensaje electrónico dirigido a otros dominios debe contener una sentencia o cláusula de confidencialidad.

Para todos los usuarios de correo electrónico, el tamaño máximo para recibir o enviar mensajes es de 25 MB (incluyendo la suma de todos los adjuntos).

Usos no aceptables del servicio

Envío de correos masivos que no hayan sido previamente autorizados a través del procedimiento formal de Solicitud de Cuentas de Usuario, establecido por la entidad.

Envío, reenvío o intercambio de mensajes no deseados o considerados como SPAM, cadena de mensajes o publicidad.

Envío o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que represente riesgo de virus.

Envío o intercambio de mensajes que promuevan la discriminación sobre la raza, nacionalidad, género, edad, estado marital, orientación sexual, religión o discapacidad, o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluidas el lavado de activos.

Envió de mensajes que contengan amenazas o mensajes violentos.

Crear, almacenar o intercambiar mensajes que atenten contra las leyes de derechos de autor.

Divulgación no autorizada de información propiedad de La Alcaldía de La Estrella.

Enviar, crear, modificar o eliminar mensajes de otro usuario sin su autorización.

Abrir o hacer uso y revisión no autorizada de la cuenta de correo electrónico de otro usuario sin su autorización.

Adulterar o intentar adulterar mensajes de correo electrónico.

Enviar correos masivos, con excepción de funcionarios con nivel de director o superior, quienes sean previamente autorizados por estos para ello, o de funcionarios que en calidad de sus funciones amerite la excepción.

Cualquier otro propósito inmoral, ilegal o diferente a los considerados en el apartado “Usos aceptable del servicio” de la presente política de seguridad de la información.

1.1.7. *POLÍTICA DE USO DE INTERNET*

Objetivo: Definir los lineamientos generales para el buen uso del internet y asegurar una adecuada protección de la información de La Alcaldía de La Estrella.

Usos aceptables del servicio

La solicitud del servicio de internet se debe hacer mediante el procedimiento formal de Creación, Edición y Eliminación de Cuentas.

Este servicio debe utilizarse exclusivamente para el desempeño de las funciones y actividades desarrolladas durante la contratación en La Alcaldía de La Estrella y no debe utilizarse para ningún otro fin.

Los usuarios autorizados para hacer uso del servicio de Internet son responsables de evitar prácticas o usos que puedan comprometer los recursos tecnológicos de La Alcaldía de La Estrella o que afecte la seguridad de la información de la misma.

Todas las comunicaciones establecidas mediante este servicio pueden ser revisadas y/o monitoreadas por el administrador del servicio o cualquier instancia de vigilancia y control.

El navegador autorizado para el uso de Internet en la red de LA ALCALDIA DE LA ESTRELLA es el instalado por el personal autorizado de la oficina de sistemas, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para prevenir ataques de virus, spyware y otro tipo de software o código malicioso.

No se permite la conexión de módems externos o internos en la red de La Alcaldía de La Estrella, previa solicitud autorizada por la Oficina de Sistemas.

El acceso a internet por cada usuario depende del rol que desempeñe en La Alcaldía de La Estrella y para los cuales este formal y expresamente autorizado.

Todo usuario es responsable de informar el acceso a contenidos o servicios no autorizados o que no correspondan al desempeño de sus funciones o actividades dentro de La Alcaldía de La Estrella.

Para realizar intercambio de información de propiedad de La Alcaldía de La Estrella con otras entidades, se debe seguir un proceso formal de retención de la información, el cual debe contar con la previa autorización del dueño de la información.

La Alcaldía de La Estrella se reserva el derecho de realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los usuarios. Así mismo, revisar, registrar y evaluar las actividades realizadas durante la navegación.

Todos los usuarios que se encuentren autorizados son responsables de dar un uso adecuado de este recurso y por ninguna razón pueden hacer uso para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la

legislación vigente, las políticas de seguridad de la información, la seguridad de la información, entre otros.

Los funcionarios, terceros, aprendices, practicantes, proveedores de La Alcaldía de La Estrella no deben asumir en nombre de La Alcaldía de La Estrella, posiciones personales en encuestas de opinión, foros u otros medios similares.

Este recurso puede ser utilizado para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de La Alcaldía de La Estrella.

Uso no aceptable del servicio

Envío o descarga de información masiva de un tamaño grande o pesado que pueda congestionar la red a menos que el desempeño de las funciones lo amerite.

Envío, descarga o visualización de información con contenidos restringidos y que atenten contra la integridad moral de las personas o instituciones.

Todos los usuarios invitados que tengan acceso al servicio de internet deben cumplir estrictamente con las políticas de seguridad de la información, de lo contrario asumirán las acciones pertinentes.
No se permite el acceso a páginas con contenido restringido como pornografía, anonimizadores, actividades criminales y/o terrorismo, crímenes computacionales, hacking, discriminación, contenido malicioso, suplantación de identidad, spyware, adware, redes peer to peer (p2p) o páginas catalogadas como de alto riesgo dictaminados de la herramienta de administración de contenidos de LA ALCALDIA DE LA ESTRELLA y las emitidas por los entes de control.

No se permite la descarga, uso, intercambio o instalación de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución, información o productos que atenten contra la propiedad intelectual, archivos ejecutables que comprometan la seguridad de la información, herramientas de hacking, entre otros.

1.1.8. *POLÍTICA DE USO DE REDES SOCIALES*

Objetivo: Definir los lineamientos generales para el uso del servicio de Redes sociales por parte de los usuarios autorizados en LA ALCALDIA DE LA ESTRELLA.

Usos aceptables del servicio

Todos los usuarios autorizados para hacer uso de los servicios de Redes Sociales son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información de La Alcaldía de La Estrella.

El servicio autorizado debe ser utilizado exclusivamente para el desarrollo de las actividades relacionadas con La Alcaldía de La Estrella. Todas las comunicaciones establecidas mediante este servicio deben ser monitoreadas por el administrador del servicio o cualquier instancia de vigilancia y control que lo requiera.

Es permitido el uso de redes sociales utilizando video conferencia y streaming (descarga de audio y video), siempre y cuando no interfiera o altere la operación normal de los sistemas de información de La Alcaldía de La Estrella.

La Alcaldía de La Estrella facilita el acceso a estas herramientas, teniendo en cuenta que constituyen un complemento de varias actividades que se realizan por estos medios y para el desempeño de las funciones y actividades a desempeñar por parte de funcionarios, terceros, aprendices, practicantes, proveedores, sin embargo, es necesario hacer buen uso de estas herramientas de forma correcta y moderada.

No se deben descargar programas ejecutables o archivos que puedan contener software o código malicioso.

No se permiten descargas, distribución de material obsceno y no autorizado, degradante, terrorista, abusivo o calumniante a través del servicio de Redes Sociales.

No se debe practicar e intentar acceder de forma no autorizada a los sistemas de seguridad del servicio de Internet de La Alcaldía de La Estrella, o aprovechar el acceso a Redes sociales para fines ilegales.

Es claro que no se puede difundir cualquier tipo de virus o software de propósito destructivo o malintencionado.

Todos los funcionarios, terceros, aprendices, practicantes, proveedores de La Alcaldía de La Estrella, deben seguir los procedimientos y planes de comunicaciones interna y externa.

La Oficina de Comunicaciones, será la encargada de determinar las directrices y lineamientos para el uso de las diferentes herramientas o plataformas de redes sociales en LA ALCALDIA DE LA ESTRELLA.

1.1.9. *POLÍTICA DE USO DE RECURSOS TECNOLÓGICOS*

Objetivo: Definir los lineamientos generales para el uso aceptable de los recursos tecnológicos de La Alcaldía de La Estrella.

Usos aceptables del servicio

La Alcaldía de La Estrella asigna los recursos tecnológicos necesarios como herramientas de trabajo para el desempeño de las funciones y actividades laborales de los funcionarios, terceros, aprendices, practicantes, proveedores de ser necesario.

El uso adecuado de estos recursos se establece bajo los siguientes criterios:

La instalación de software se encuentra bajo la responsabilidad la Oficina de Sistemas y por tanto son los únicos autorizados para realizar esta actividad.

Ningún usuario debe realizar cambios relacionados con la configuración de los equipos, como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo. Estos cambios únicamente deben ser realizados por la Oficina de Sistemas de La Alcaldía de La Estrella.

La Oficina de Sistemas es la responsable de definir la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas en La Alcaldía de La Estrella para ser instaladas en las estaciones de trabajo de los usuarios; así mismo, realizará el control y verificación del cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

Sólo el personal autorizado por la Oficina Sistemas podrá realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de La Alcaldía de La Estrella; las conexiones establecidas para este fin utilizan los esquemas de seguridad establecidos por La Alcaldía de La Estrella.

Los funcionarios, terceros, aprendices, practicantes, proveedores de La Alcaldía de La Estrella son responsables de hacer buen uso de los recursos tecnológicos y en ningún momento pueden ser usados para beneficio propio o para realizar prácticas ilícitas o mal intencionadas que atenten contra otros funcionarios, terceros, aprendices, practicantes, proveedores, legislación vigente y políticas y lineamientos de seguridad de la información establecidas por la Entidad.

La información clasificada como personal almacenada en los equipos de cómputo, medios de almacenamiento o cuentas de correo institucionales, deben ser guardadas en su totalidad en una carpeta especificada para tal fin, la cual debe ser nombrada como “PERSONAL”.

Todo activo de propiedad de La Alcaldía de La Estrella, asignado a un funcionario, terceros, aprendices, practicantes, proveedores de la misma, debe ser entregado al finalizar el vínculo laboral o contractual o por cambio de cargo si es necesario.

Esto incluye los documentos corporativos, equipos de cómputo (Hardware y Software), dispositivos móviles, tarjetas de acceso, manuales, tarjetas de identificación y la información que tenga almacenada en dispositivos móviles o removibles.

1.1.11. *POLÍTICA DE GESTIÓN DE MEDIOS DE ALMACENAMIENTO*

Objetivo: Proteger la información de LA ALCALDIA DE LA ESTRELLA velando por la protección de la confidencialidad, integridad y disponibilidad de la información que se encuentra en unidades de almacenamiento.

Gestión y Disposición de medios removibles

Todos los dispositivos y unidades de almacenamiento removibles, tales como cintas, CD's, DVD's, dispositivos personales "USB", discos duros externos, cámaras fotográficas, cámaras de video, celulares, entre otros, deben ser controlados desde su acceso a la red de La Alcaldía de La Estrella y uso hasta finalización de su contrato o cese de actividades.

Toda la información clasificada como CONFIDENCIAL o RESERVADA que sea almacenada en medios removibles y que se requiera de protección especial, debe cumplir con las directrices de seguridad emitidas por la Oficina sistemas, específicamente aquellas referentes al empleo de técnicas de cifrado.

Se debe llevar el registro de todos los medios removibles de La Alcaldía de La Estrella y mantenerlos actualizados.

Todos los medios removibles deben ser almacenados de manera segura.

La Oficina de Sistemas puede restringir que medios de almacenamiento removibles se conecten a los equipos de cómputo que sean propiedad de La Alcaldía de La Estrella o que estén bajo su custodia, y puede llevar a cabo cualquier acción de registro o restricción, con el fin de evitar fuga de información a través de medios removibles.

Los medios de almacenamiento removibles que se conecten a la red de datos de entidad o que se encuentren bajo su custodia, están sujetos a monitoreo por parte de la Oficina de Sistemas.

Todos los retiros de medios de almacenamiento de las instalaciones de La Alcaldía de La Estrella, como discos duros externos, se deben realizar con la autorización del propietario del proceso misional, estratégico, mejora continua o de

apoyo, definidos de acuerdo con el mapa de procesos de La Alcaldía de La Estrella, a través del formato orden de salida de elementos.

Todos los medios de almacenamiento removibles propiedad de La Alcaldía de La Estrella, deben estar almacenados en un ambiente seguro acorde con las especificaciones del fabricante.

Se debe hacer seguimiento a los medios de almacenamiento removibles como Discos Duros, Cintas, etc., con el fin de garantizar que la información sea transferida a otro medio antes de que esta quede inaccesible por deterioro o el desgaste que sufren a causa de su vida útil.

Borrado seguro

Todos los medios de almacenamiento que Sean de propiedad de terceros y que estén autorizados por La Alcaldía de La Estrella para su uso dentro de la red corporativa, deben contar con su respectivo soporte.

Todos los medios de almacenamiento que contengan información de La Alcaldía de La Estrella y que salgan de la misma y que no se les vaya a dar más uso, deben seguir el procedimiento de borrado seguro definido por La Alcaldía de La Estrella, el cual garantiza que la información no es recuperable (Aplica para medios de almacenamiento de equipos alquilados, equipos para pruebas de concepto, equipos de proveedores y/o contratistas, discos duros externos, etc.).

Los medios de almacenamiento que contengan información de La Alcaldía de La Estrella y que vayan a ser dados de baja o reutilizados, deben seguir el procedimiento de borrado seguro definido por la entidad, el cual garantiza que la información no se es recuperable (Aplica para medios de almacenamiento externos o de equipos que son reasignados, formateados, reinstalados o que por degaste o falla son retirados o dados de baja).

Eliminar de forma segura (destrucción o borrado) los medios de almacenamiento que no se utilicen y que contengan información de La Alcaldía de La Estrella.

Transferencia de Medios Físicos

Toda la información clasificada como CONFIDENCIAL o RESERVADA que se desee almacenar en medios removibles y que sean transportados fuera de las instalaciones de La Alcaldía de La Estrella, debe cumplir con las disposiciones de seguridad indicadas por la Oficina de Sistemas, específicamente aquellas referentes al empleo de técnicas de cifrado.

El transporte de los medios físicos se debe hacer mediante un medio de transporte confiable y seguro, tomando las medidas y precauciones necesarias

para garantizar que los medios de almacenamiento sean transportados adecuadamente, de esta forma se evita una afectación a la integridad y disponibilidad de la información que reposa en el medio.

Se debe llevar un registro de custodia de los medios de almacenamiento físico que son transportados.

1.1.12. *POLÍTICA DE CONTROL DE ACCESO*

Objetivo: Definir las directrices generales para un acceso controlado a la información de La Alcaldía de La Estrella.

Control de Acceso a Redes y Servicios en Red

La Alcaldía de La Estrella a través de la oficina de Sistemas suministra a los funcionarios y/o usuarios las contraseñas de acceso a los servicios de red, servicios y sistemas de información que requiera para el desempeño de sus funciones laborales.

Las claves son de uso personal e intransferible y es responsabilidad del usuario el uso de las credenciales asignadas.

Sólo el personal designado por la Oficina de Sistemas está autorizado para instalar software o hardware en los equipos, servidores e infraestructura de tecnología de La Alcaldía de La Estrella.

Toda actividad que requiera acceder a los servidores, equipos o a las redes de La Alcaldía de La Estrella, se debe realizar en las instalaciones. No se debe realizar ninguna actividad de tipo remoto sin la debida autorización de la Oficina de Sistemas y Jefe de Despacho que requiera el servicio.

La conexión remota a la red de área local de La Alcaldía de La Estrella debe ser establecida a través de una conexión VPN segura aprovisionada por La Alcaldía de La Estrella, la cual debe ser autorizada por la Oficina de Sistemas, que cuenta con el monitoreo y registro de las actividades necesarias.

La creación y retiro de usuarios en los sistemas de información en producción debe seguir un procedimiento de Creación, Edición y Eliminación de Usuarios.

Mediante el registro de eventos en los diversos componentes de la plataforma tecnológica, se efectúa el seguimiento a los accesos realizados por los usuarios, con el fin de minimizar los riesgos de pérdida de integridad, disponibilidad y confidencialidad de la información.

Gestión de Acceso a Usuarios

Se establece el uso de contraseñas individuales para determinar las responsabilidades de su administración.

Los usuarios pueden elegir y cambiar sus claves de acceso periódicamente, inclusive antes de que la cuenta expire.

Las contraseñas deben contener Mayúsculas, Minúsculas, números y por lo menos un carácter especial y de una longitud mayor a 8 caracteres.

El sistema debe obligar al usuario a cambiar la contraseña por lo mínimo 1 vez cada 45 días.

Todos los usuarios en su primer inicio de sesión deben cambiar las contraseñas suministrada por la mesa de soporte técnico.

Todos los usuarios deben dar buen uso a las claves de acceso suministradas y no deben escribirlas o dejarlas a la vista.

Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.

Cambiar todas las claves de acceso que vienen predeterminadas por el fabricante, una vez instalado y configurado el software y el hardware (por ejemplo, apliance, impresoras, routers, switch, herramientas de seguridad, etc.).

El acceso a los equipos especializados por medio de la red debe establecerse por medio de métodos de autenticación con protocolos de seguridad.

No prestar, divulgar o difundir la contraseña de acceso asignadas a compañeros, jefes u otras personas que lo soliciten, pues estas son de carácter personal e intransferible, o compartir previa autorización de la oficina de Sistemas y o Secretaria de Despacho.

Todos los usuarios deben dar cumplimiento a las políticas de seguridad de la información de uso y selección de las contraseñas de acceso, por lo tanto, son responsables de cualquier acción que se realice utilizando el usuario y contraseña asignados.

Las contraseñas no deben ser reveladas por vía telefónica, correo electrónico o por ningún otro medio.

Reportar a la Oficina de Sistemas sobre cualquier incidente o sospecha de que otra persona esté utilizando su contraseña o usuario asignado.

Reportar a la Oficina de Sistemas sobre cualquier sospecha o evidencia de que una persona esté utilizando una contraseña y usuario que no le pertenece.

Las contraseñas de acceso a los servidores y administración de los Sistemas de Información deben ser cambiadas mínimo cada un (1) mes.

El acceso a Bases de Datos, Servidores y demás componentes tecnológicos de administración de la Plataforma y Sistemas de Información, debe estar autorizado por la Oficina de Sistemas.

Revisión de los derechos de acceso de los Usuarios

Los derechos de acceso de los usuarios a la información y a la Plataforma Tecnológica y de procesamiento de información de La Alcaldía de La Estrella, debe ser revisada periódicamente y cada vez que se realicen cambios de personal en los procesos o grupos de trabajo.

Retiro de los derechos de acceso

Cada uno de los procesos que hacen parte del Sistema de Gestión de Calidad de La Alcaldía de La Estrella es responsable de comunicar a la Oficina de Talento Humano, el cambio de cargo, funciones o actividades o la terminación contractual de los Colaboradores pertenecientes al proceso. La Oficina de Talento Humano y Gestión Contractual son las encargadas de comunicar a la Oficina de Sistemas sobre estas novedades, con el fin de retirar los derechos de acceso a los servicios informáticos y de procesamiento de información.

1.1.13. POLÍTICA SEGURIDAD FÍSICA Y DEL ENTORNO

Objetivo: Evitar accesos físicos no autorizados a las instalaciones de procesamiento de información, que atenten contra la confidencialidad, integridad o disponibilidad de la información de La Alcaldía de La Estrella.

Los visitantes deben permanecer acompañados de un funcionario o Colaborador de La Alcaldía de La Estrella, cuando se encuentren en las oficinas o áreas donde se maneje información.

Los visitantes que requieran permanecer en las oficinas de La Alcaldía de La Estrella por periodos superiores a dos (2) días deben ser presentados al personal de oficina donde permanecerán.

El horario autorizado para recibir visitantes en las instalaciones de La Alcaldía de La Estrella es de 7:30 AM a 12:30 PM y de 1:30 PM a 5:30 PM. En horarios

distintos se requerirá de la autorización del jefe de despacho o líder correspondiente.

Los dispositivos removibles, así como toda información CONFIDENCIAL de LA ALCALDIA DE LA ESTRELLA, independientemente del medio en que se encuentre almacenada, deben permanecer guardados bajo seguridad durante horario no hábil o en horarios en los cuales los funcionarios, terceros, aprendices, practicantes, proveedores responsables no se encuentren en su sitio de trabajo.

Ubicación y Protección de los equipos.

La plataforma tecnológica (Hardware, software y comunicaciones) debe contar con las medidas de protección física y eléctrica, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados.

Se debe instalar sistemas de protección eléctrica en el centro de cómputo y comunicaciones de manera que se pueda interrumpir el suministro de energía en caso de emergencia. Así mismo, se debe proteger la infraestructura de procesamiento de información mediante contratos de mantenimiento y soporte.

Seguridad de los equipos fuera de las instalaciones

En caso de pérdida o robo de un equipo portátil se debe informar inmediatamente al a la Oficina de Sistemas y debe poner la denuncia ante las autoridades competentes y debe hacer llegar copia de esta.

Para el caso de los equipos que cuentan con puertos de transmisión y recepción de infrarrojo y Bluetooth estos deben estar deshabilitados.

Todos los equipos de cómputo deben ser registrados al ingreso y al retirarse de las instalaciones de La Alcaldía de La Estrella.

Seguridad en la reutilización o eliminación de los equipos

Cuando un equipo de cómputo sea reasignado o dado de baja, se debe realizar una copia de respaldo de la información que se encuentre almacenada. Posteriormente debe ser sometido al procedimiento de borrado seguro de la información y del software instalado, con el fin de evitar pérdida de la información o recuperación no autorizada de la misma.

Retiro de Activos

Ningún equipo de cómputo, información o software debe ser retirado de La Alcaldía de La Estrella sin una autorización formal.

Se debe realizar periódicamente comprobaciones puntuales para detectar el retiro no autorizado de activos de La Alcaldía de La Estrella.

1.1.14. *POLÍTICA DE ESCRITORIO DESPEJADO Y PANTALLA DESPEJADA*

Objetivo: Definir los lineamientos generales para mantener el escritorio y la pantalla despejada, con el fin de reducir el riesgo de acceso no autorizado, pérdida y daño de la información de La Alcaldía de La Estrella.

Todo el personal de La Alcaldía de La Estrella debe conservar su escritorio libre de información propia de la Entidad, que pueda ser copiada, utilizada o estar al alcance de terceros o por personal que no tenga autorización para su uso o conocimiento.

Todo el personal de La Alcaldía de La Estrella debe bloquear la pantalla de su equipo de cómputo cuando no estén haciendo uso de ellos o que por cualquier motivo deban dejar su puesto de trabajo.

Todos los usuarios al finalizar sus actividades diarias deben salir de todas las aplicaciones y apagar las estaciones de trabajo.

Al imprimir documentos de carácter CONFIDENCIAL, estos deben ser retirados de la impresora inmediatamente. Así mismo, no se deben reutilizar papel que contenga información CONFIDENCIAL.

En horario no hábil o cuando los lugares de trabajo se encuentren desatendidos, los usuarios y/o funcionarios deben dejar la información CONFIDENCIAL protegida bajo llave.

1.1.15. *POLÍTICA DE GESTIÓN DE CAMBIOS*

Objetivo: Asegurar que los cambios a nivel de infraestructura, aplicaciones y sistemas de información realizados en La Alcaldía de La Estrella se realicen de forma controlada.

Se deben establecer procedimientos para el control de cambios ejecutados en La Alcaldía de La Estrella. Toda solicitud de cambio en los servicios de procesamiento de información de La Alcaldía de La Estrella se debe realizar siguiendo el Procedimiento de gestión de cambios, con el fin de asegurar la planeación del cambio y evitar una afectación a la disponibilidad, integridad o confidencialidad de la información.

Se debe llevar una trazabilidad del control de cambios solicitados.

En el procedimiento de gestión de cambios se debe especificar los canales autorizados para la recepción de solicitudes de cambios, como la Mesa de soporte técnico, correo electrónico o un oficio dirigido al Líder Sistemas.

Se debe establecer y aplicar el procedimiento formal para la aprobación de cambios sobre sistemas de información existentes, como actualizaciones, aplicación de parches o cualquier otro cambio asociado a la funcionalidad de los sistemas de información y componentes que los soportan, tales como el sistema operativo o cambios en hardware.

Se deben especificar en qué momento existen cambios de emergencia en la cual se debe garantizar que los cambios se apliquen de forma rápida y controlada.

Los cambios sobre sistemas de información deben ser planeados para asegurar que se cuentan con todas las condiciones requeridas para llevarlo a cabo de una forma exitosa y se debe involucrar e informar a los funcionarios, terceros, aprendices, practicantes, proveedores que por sus funciones tienen relación con el sistema de información.

Previo a la aplicación de un cambio se deben evaluar los impactos potenciales que podría generar su aplicación, incluyendo aspectos funcionales y de seguridad de la información, estos impactos se deben considerar en la etapa de planificación del cambio para poder identificar acciones que reduzcan o eliminen el impacto.

Los cambios realizados sobre sistemas de información deben ser probados para garantizar que se mantiene operativo el sistema de información, incluyendo aquellos aspectos de seguridad de la información del sistema y que el propósito del cambio se cumplió satisfactoriamente.

1.1.16. *POLÍTICA DE SEPARACIÓN DE AMBIENTES DE DESARROLLO, PRUEBAS Y PRODUCCIÓN*

Objetivo: Reducir riesgos asociados a modificaciones, alteraciones, cambios o accesos no autorizados en sistemas en producción de La Alcaldía de La Estrella.

LA ALCALDIA DE LA ESTRELLA debe establecer y mantener ambientes separados de Desarrollo, Pruebas y Producción, dentro de la infraestructura de Desarrollo de Sistemas de Información de La Alcaldía de La Estrella. Esto aplica para sistemas que contengan información catalogada con criticidad alta de acuerdo con el inventario y clasificación de activos de información.

El ambiente de desarrollo se debe utilizar para propósitos de implementación, modificación, ajuste y/o revisión de código. Por su parte, el ambiente de pruebas se debe utilizar para realizar el conjunto de validaciones funcionales y

técnicas del software, aplicación o sistema de información, teniendo como base los criterios de aceptación y los requerimientos de desarrollo. Por último, el ambiente de producción debe utilizarse para la prestación de un servicio que involucra el manejo de datos reales y que tiene un impacto directo sobre las actividades realizadas como parte de un proceso de La Alcaldía de La Estrella.

En la Entidad territorial se debe seguir un procedimiento formal para el paso de software, aplicaciones y sistemas de información de un ambiente a otro (desarrollo, pruebas y producción), donde se establecen las condiciones a seguir para alcanzar la puesta en producción de un sistema nuevo o la aplicación de un cambio a uno existente. Esto aplica para sistemas que contengan información catalogada con criticidad alta de acuerdo con el inventario y clasificación de activos de información.

No se deben realizar pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción. Esto puede conducir a fraude o inserción de código malicioso.

En los ambientes de desarrollo y pruebas no se deben utilizar datos reales del ambiente de producción, sin antes haber pasado por un proceso de ofuscamiento.

Se debe restringir e l acceso a compiladores, editores y otros utilitarios del sistema operativo en el ambiente de producción, cuando no sean indispensables para el funcionamiento de este.

Se deben utilizar controles de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas.

Las interfaces de los sistemas deben ser identificadas claramente para poder determinar a qué instancia se está realizando la conexión.

Los ambientes deben estar claramente identificados, para evitar así confusiones en la aplicación de tareas o en la ejecución de procesos propios de cada uno.

Los cambios a sistemas en producción que involucren aspectos funcionales deben ser informados y consultados con el(los) proceso (s) propietario(s) de la información.

Se debe establecer una guía para el Desarrollo seguro de Software en La Alcaldía de La Estrella.

1.1.17. *POLÍTICA DE PROTECCIÓN CONTRA CÓDIGO MALICIOSO*

Objetivo: Definir las medidas de prevención, detección y corrección frente a las amenazas causadas por códigos maliciosos en La Alcaldía de Las Estrella.

Toda la infraestructura de procesamiento de información de LA ALCALDIA DE LA ESTRELLA cuenta con un sistema de detección y prevención de intrusos, herramienta de Anti-Spam y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos.

Se debe restringir la ejecución de aplicaciones y mantener instalado y actualizado el antivirus, en todas las estaciones de trabajo y servidores de La Alcaldía de La Estrella.

Se debe restringir la ejecución de código móvil, aplicando políticas a nivel de sistemas operativos, navegadores y servicio de control de navegación.

Todos los funcionarios, terceros, aprendices, practicantes, proveedores que hacen uso de los servicios de tecnología de la información y comunicaciones de La Alcaldía de La Estrella son responsables del manejo del antivirus para analizar, verificar y (si es posible) eliminar virus o código malicioso de la red, el computador, los dispositivos de almacenamiento fijos, removibles, archivos, correo electrónico que estén utilizando para el desempeño de sus funciones laborales.

La Alcaldía de La Estrella cuenta con el software necesario como antivirus para protección a nivel de red y de estaciones de trabajo, contra virus y código malicioso, el servicio es administrado por la Oficina de Sistemas de La Alcaldía de La Estrella.

Los antivirus adquiridos por La Alcaldía de La Estrella, sólo debe ser instalados por los responsables de la Oficina de Sistemas.

Los equipos de terceros que son autorizados para conectarse a la red de datos de La Alcaldía de La Estrella deben tener antivirus y contar con las medidas de seguridad apropiadas.

Todos los equipos conectados la red de La Alcaldía de La Estrella pueden ser monitoreados y supervisados por la Oficina de Sistemas.

Se debe mantener actualizado a sus últimas versiones funcionales las herramientas de seguridad, incluido, motores de detección, bases de datos de firmas, software de gestión del lado cliente y del servidor, etc.

Se debe hacer revisiones y análisis periódicos del uso de software no malicioso en las estaciones de trabajo y servidores. La actividad debe ser programada de forma automática con una periodicidad semanal y su correcta ejecución y revisión estará a cargo de la Oficina de Sistemas.

La Alcaldía de La Estrella debe contar con controles para analizar, detectar y restringir el software malicioso que provenga de descargas de sitios web de

baja reputación, archivos almacenados en medios de almacenamiento removibles, contenido de correo electrónico, etc.

Se deben hacer campañas de sensibilización a todos los funcionarios, terceros, aprendices, practicantes, proveedores de ser el caso de La Alcaldía de La Estrella, con el fin de generar una cultura de seguridad de la información.

Los funcionarios, terceros, aprendices, practicantes, proveedores de LA ALCALDIA DE LA ESTRELLA pueden iniciar en cualquier momento un análisis bajo demanda de cualquier archivo o repositorio que consideren sospechoso de contener software malicioso. En cualquier caso, los funcionarios, terceros, aprendices, practicantes, proveedores cuando sea necesario siempre podrán consultar a la Oficina de Sistemas sobre el tratamiento que debe darse en caso de sospecha de programa maligno.

Los usuarios no podrán desactivar o eliminar la suite de productos de seguridad, incluidos los programas antivirus o de detección de código malicioso, en los equipos o sistemas asignados para el desempeño de sus funciones laborales.

Todo usuario es responsable por la destrucción de archivos o mensajes, que le haya sido enviado por cualquier medio provisto por La Alcaldía de La Estrella, cuyo origen le sea desconocido o sospechoso y asume la responsabilidad de las consecuencias que puede ocasionar su apertura o ejecución. En estos casos no se deben contestar dichos mensajes, ni abrir los archivos adjuntos, el usuario debe reenviar el correo a la cuenta sistemas@laestrella.gov.co.

El único servicio de antivirus autorizado en La Alcaldía de La Estrella es el asignado directamente por la Oficina de Sistemas, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para evitar ataques de virus, spyware y otro tipo de software malicioso. Además, este servicio tiene diferentes procesos de actualización que se aplican de manera periódica y segura. Excepcionalmente se podrá realizar la ejecución de otro programa antivirus, únicamente por personal autorizado por la Oficina de Sistemas, a efectos de reforzar el control de presencia o programación de virus o código malicioso.

La Oficina de Sistemas es el responsable de administrar la plataforma tecnológica que soporta el servicio de Antivirus para los equipos de cómputo conectados a la red de La Alcaldía de La Estrella.

La Oficina de Sistemas se reserva el derecho de monitorear las comunicaciones y/o la información que se generen, comuniquen, transmitan o trasporten y almacenen en cualquier medio, en busca de virus o código malicioso.

La Oficina de Sistemas se reserva el derecho de filtrar los contenidos que se trasmitan en la red de La Alcaldía de La Estrella, con el fin de evitar amenazas de virus.

Todos los correos electrónicos serán revisados para evitar que tengan virus. Si el virus no puede ser eliminado, la información será borrada.

1.1.18. *POLÍTICA DE BACKUP*

Objetivo: Proporcionar medios de respaldo de información adecuados para La Alcaldía de La Estrella, para asegurar la información crítica y que el software asociado se pueda recuperar después de una falla.

La Oficina de Sistemas, debe realizar periódicamente un análisis de las necesidades de la entidad para determinar la información crítica que debe ser respaldada y la frecuencia con que se debe realizar.

La Oficina de Sistemas y el responsable asignado junto a los propietarios de la información deben determinar los requerimientos para respaldar la información y los datos en función de su criticidad, para lo cual se debe elaborar y mantener el inventario de activos de TI (Tecnologías de la Información)

La Oficina de Sistemas debe disponer y controlar la ejecución de las copias, así como la prueba periódica de su restauración. Para esto se debe contar con instalaciones de respaldo que garanticen la disponibilidad de toda la información y del software crítico de La Alcaldía de La Estrella.

Se debe definir y documentar un esquema de respaldo de la información.

El dueño de la información es responsable de definir claramente el periodo de retención de respaldos, en función de los requerimientos de las áreas funcionales.

Se debe verificar periódicamente, la integridad de las copias de respaldo que se están almacenando, con el fin de garantizar la integridad y disponibilidad de la información.

Se deben definir procedimientos para el respaldo de la información, que incluyan los siguientes parámetros: (van viñetas)?

Establecer un esquema de rotulado de las copias de respaldo, que contengan toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.

Definir el procedimiento de reemplazo de los medios de almacenamiento de copias de respaldo, una vez terminada la posibilidad de ser reutilizados de acuerdo

con lo indicado por el proveedor, y asegurar la destrucción de los medios de información retirados o desechados.

Almacenar en una ubicación remota o externa las copias de respaldo recientes de información, junto con registros completos de las mismas y sus procedimientos documentados de restauración.

Se deben asignar los niveles de protección física y ambiental adecuada a la información de respaldo según las normas aplicadas y las especificaciones dadas por el fabricante.

Se deben extender los mismos controles de seguridad aplicados a los activos de TI en el sitio principal al sitio alterno.

La Oficina de Sistemas, a través del Administrador de Bases de Datos, sistemas de información, servicios de Red y servidores, debe:

Actualizar periódicamente las configuraciones de los Servidores para la correcta ejecución de las copias de respaldo.

Efectuar las copias de información de los Servidores, cada vez que se realice un cambio significativo en los Sistemas Operativos o configuraciones Básicas.

Realizar una copia de respaldo incremental diaria de los Servidores de Base de Datos, servidores Web, Sistemas de Información misionales, Aplicaciones, Desarrollo y dispositivos de red.

Realizar un respaldo Diferencial semanalmente de los Servidores de Base de Datos, servidores Web, Sistemas de Información, Aplicaciones, Desarrollo y dispositivos de red.

Las copias de respaldo se deben realizar en horario no hábil, lo cual será verificado a través de Procesos Automáticos.

Una vez se verifique la correcta ejecución de las copias de respaldo, se debe retirar el medio de Backup.

Los dispositivos magnéticos que contienen información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra almacenada.

El sitio alterno donde se almacenan las copias de respaldo debe contar con los controles de seguridad necesarios, para cumplir con las medidas de protección y seguridad física apropiados.

Conservar los medios de almacenamiento de información en un ambiente que cuente con las especificaciones emitidas por los fabricantes o proveedores.

La Oficina de Sistemas, debe contar con un juego de medios de Backup necesarios por cada Servidor en el sitio Externo.

La Oficina de Sistemas, cuenta con un responsable para gestionar la entrega o retiro de las copias de Backup del sitio externo.

Las copias de Backup con la Información actualizada, no deben permanecer más de una semana fuera del sitio externo.

Registro de Respaldo de Información

Llevar el registro de los Respaldos de Información realizada de forma Diaria.
Registro del retiro de los medios de Backup del sitio externo.
Registro del ingreso de los medios de Backup al sitio externo.
Inventario de los medios de Backup.
Comprobación de Integridad de la Información

La información respaldada debe ser probada como mínimo dos veces al año, asegurando que es confiable, integra y que se estará disponible en el evento que se requiera para su utilización en casos de emergencia.

Se deben probar los procedimientos de restauración, para asegurar que son efectivos y que pueden ser ejecutados en los tiempos establecidos.

Se debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información.

Restaurar por lo menos cada seis meses, el escenario adecuado para probar las copias de respaldo de los Servidores.

Configurar la herramienta de ejecución de copias de respaldo para que automáticamente registre el éxito o errores en la ejecución.

Validar la integridad y accesibilidad de las cintas magnéticas por lo menos cada cuatro meses.

Mantener siempre una copia de la información de los Servidores, por lo menos con una antigüedad no superior a 24 horas.

Se debe mantener un monitoreo frecuente sobre el rendimiento y alcance de la información en la Base de Datos para así asegurar la integridad de la información respaldada.

Respaldo de Información para Usuarios Finales

Todos los usuarios son responsables de realizar los respaldos de información personal almacenada en los equipos asignados.

La Oficina de Sistemas, debe mantener los respaldos de información en condiciones adecuadas de medio ambiente, temperatura, humedad, y otros.

Ningún usuario puede realizar copias de respaldo en sus dispositivos de almacenamiento removibles personales, ya que esto puede ser denominado fuga de información.

Todos los funcionarios, terceros, aprendices, practicantes, proveedores de LA ALCALDIA DE LA ESTRELLA deben dar estricto cumplimiento a esta política de seguridad de la información y el que haga caso omiso puede ser sujeto a acciones disciplinarias o civiles, incluyendo la terminación del respectivo contrato.

Se debe elaborar un plan de emergencia para todas las aplicaciones que manejen información crítica de La Alcaldía de La Estrella, el responsable de la información debe asegurar que el plan es adecuado, frecuentemente actualizado y periódicamente probado y revisado.

1.1.19. *POLÍTICA DE EVENTOS DE AUDITORIA*

Objetivo: Asegurar que los registros de los eventos y las operaciones realizadas sobre los sistemas de información y plataforma tecnología de La Alcaldía de La Estrella permitan contar con evidencia necesaria para la gestión de incidentes de seguridad de la información.

Registro de eventos

Todos los accesos de usuarios a los sistemas, redes de datos y aplicaciones de La Alcaldía de La Estrella, deben ser registrados.

Se deben habilitar los logs de eventos requeridos y deben ser revisados con regularidad. Se debe hacer copia de respaldo de información de los eventos de auditoria, ya que en caso de un incidente de seguridad de la información deben estar disponibles.

Registro del administrador y del Operador

Todas las actividades de operación realizadas por los administradores de la infraestructura de procesamiento de información de La Alcaldía de La Estrella deben estar debidamente registradas.

Los administradores de la infraestructura tecnológica y de procesamiento de información deben tener asignada una cuenta de usuario exclusiva, a través de la cual se realizarán las actividades de administración y debe ser entregada a través de un proceso formal.

Sincronización de relojes

Todos los relojes de la infraestructura de procesamiento de información de LA ALCALDIA DE LA ESTRELLA deben estar sincronizados con la hora legal colombiana.

1.1.20. *POLÍTICA DE GESTIÓN DE SEGURIDAD DE LAS REDES*

Objetivo: Establecer los controles necesarios para proteger la información de LA ALCALDIA DE LA ESTRELLA transportada desde la red interna.

La Oficina de Sistemas es la responsable de administrar y gestionar la red de LA ALCALDIA DE LA ESTRELLA.

La Oficina de Sistemas es la responsable de establecer los controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de mantener los niveles de seguridad apropiados.

LA ALCALDIA DE LA ESTRELLA proporciona a los funcionarios, terceros, aprendices, practicantes, proveedores todos los recursos tecnológicos de conectividad necesarios para que puedan desempeñar las funciones y actividades laborales, por lo cual no es permitido conectar a las estaciones de trabajo o a los puntos de acceso de la red corporativa, elementos de red (tales como switches, enrutadores, módems, etc.) que no sean autorizados por la Oficina de Sistemas de la entidad.

El trabajo a través de medios remotos a la red de datos de LA ALCALDIA DE LA ESTRELLA, sólo se permitirá de acuerdo con la Política de Teletrabajo establecida por La Alcaldía de La Estrella.

Separación de las Redes

LA ALCALDIA DE LA ESTRELLA debe establecer un esquema de segregación de redes, con el fin de controlar el acceso a los diferentes segmentos de red y garantizar la confidencialidad, integridad y disponibilidad de la información.

Se deben seguir los procedimientos de acceso o retiro de componentes tecnológicos para la solicitud de servicios de red.

Se deben establecer parámetros técnicos para la conexión segura de la red con los servicios de red.

Se deben establecer mecanismos de autenticación seguros para el acceso a la red.

Se deben separar las redes inalámbricas de las redes internas, para garantizar los principios de la seguridad de la información.

1.1.21. *POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES*

Objetivos: Establecer los criterios de seguridad para la información accedida por los proveedores.

Consideraciones de seguridad en los acuerdos con terceras partes y/o contratistas

En todos los Contratos o Acuerdos con terceras partes, que implique un intercambio, uso o procesamiento de información de La Alcaldía de La Estrella, se deben realizar Acuerdos de Confidencialidad sobre el manejo de la información.

Los Acuerdos de confidencialidad de la información deben hacer parte integral de los contratos o documentos que legalicen la relación de la entidad.

Dentro del contrato o acuerdo se deben definir claramente el tipo de información que se va a intercambiar por las partes.

1.1.22. *POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN*

Objetivo: Gestionar todos los incidentes de seguridad de la información reportados en LA ALCALDIA DE LA ESTRELLA, adecuadamente, dando cumplimiento a los procedimientos establecidos.

Reporte sobre los eventos y las debilidades de la seguridad de la información

Todos los funcionarios, terceros, aprendices, practicantes, proveedores de La Alcaldía de La Estrella y terceras partes tienen la responsabilidad de reportar de forma inmediata los eventos, incidentes o debilidades en cuanto a la seguridad de la información que identifiquen o se presenten.

Se debe dar un tratamiento adecuado a todos los incidentes de seguridad de la información reportados.

Se deben establecer las responsabilidades en la Gestión de Incidentes de Seguridad de la Información.

Se debe definir el procedimiento de atención de incidentes de seguridad de la información de LA ALCALDIA DE LA ESTRELLA.

Se debe llevar una bitácora de los incidentes de seguridad de la información reportados y atendidos.

Se debe recolectar las evidencias (Policía, Fiscalía, COLCERT, MINTIC) necesarias lo más pronto posible después del reporte del incidente.

Escalar los incidentes a niveles superiores en caso de que sea requerido.

Se debe hacer evaluaciones de los incidentes presentados ya que se puede necesitar de controles adicionales.

Para el transporte de elementos, se debe llevar la cadena de custodia.

Se deben documentar todos los incidentes de seguridad reportados.

Se debe realizar sensibilización a todos los usuarios sobre incidentes de seguridad de la información.

1.1.23. *POLÍTICA DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO*

Objetivo: Garantizar que los planes de continuidad de negocios se ejecuten de forma segura sin exponer la información de LA ALCALDIA DE LA ESTRELLA.

LA ALCALDIA DE LA ESTRELLA debe establecer los requisitos necesarios de seguridad de la información y la continuidad de la operación en caso de situaciones adversas, como desastres naturales o crisis.

Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones y responsabilidades relacionados con el plan, deben estar incorporados y definidos en los Planes de contingencias.

1.2. POLITICA DE GESTIÓN DOCUMENTAL

Esta política está relacionada con el manual del Programa de Gestión Documental (PGD) 2019-2020 de La Alcaldía de La Estrella, para lo cual se tuvieron en cuenta las directrices definidas y adoptadas en el mencionado programa y en la Resolución No. 01920 del 26 de septiembre de 2019, en el cual

se establecen los componentes mínimos que debe incorporar. Dicha política fue aprobada por el Comité interno de archivo municipal.

MANUAL DE POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

Normatividad:

Decreto Reglamentario 1377 del 27 de junio de 2013 “Por el cual se reglamenta parcialmente la Ley 1581 de 2012

Ley 1266 del 31 de diciembre de 2008 “Por la cual se dictan las disposiciones generales del Habeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y proveniente de terceros países y se dictan otras disposiciones”.

Ley 1581 del 17 de octubre 2012 “Por el cual se dictan disposiciones generales para la protección de datos personales”.

Ley 1712 del 6 de marzo de 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”.

Decreto Reglamentario 103 de 2015 “Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones”.

Definiciones

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

Aviso de privacidad: comunicación verbal o escrita generada por el responsable, dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.

Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Dato semiprivado: Es semiprivado el dato que no tiene naturaleza intima, reservada, ni publica y cuyo conocimiento y divulgación puede interesar no sólo a

su titular sino a cierto sector o grupo de personas, o a la sociedad en general, como el dato financiero y crediticio.

Dato privado: Es el dato que por su naturaleza intima o reservada solo es relevante para el titular.

Datos sensibles: Aquellos datos 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 garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Tratamiento: Se refiere a cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Habeas Data y Protección de Dato Personal: Derecho Constitucional Fundamental regulado en el artículo 15 de la Constitución Política de Colombia de 1991, el cual señala que "*Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución"*. El Habeas Data y la Protección del Dato Personal, son Derechos Fundamentales de carácter inalienable e irrenunciable de toda persona y como tal debe respetársele, tutelándose la libertad, el derecho a la autodeterminación, a la honra y a la intimidad.

Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento.

Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de estos.

Titular: Persona natural cuyos datos personales sean objeto de Tratamiento.

Información: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los responsables y/o encargados del tratamiento generen, obtengan, adquieran, transformen o controlen.

Información pública: Es toda información que el responsable y/o encargado del tratamiento, genere, obtenga, adquiera, o controle en su calidad de tal.

Información pública clasificada: Es aquella información que estando en poder de un sujeto responsable en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica, por lo 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 la ley.

Información pública reservada: Es aquella información que estando en poder de un sujeto responsable en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos.

Documento de Archivo: Es el registro de información producida o recibida por una entidad pública o privada debido a sus actividades o funciones.

Datos abiertos: Son todos aquello 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.

Principios Generales para el Tratamiento de Datos Personales

En el desarrollo, interpretación y aplicación de la Ley 1581 de 2012 y las normas que la complementan, modifican o adicionan, la Alcaldía de La Estrella aplicará de manera armónica e integral los siguientes principios rectores:

- ✓ Principio de máxima publicidad para titular universal: Toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal, de conformidad con la Ley.
- ✓ Principio de legalidad: La recolección, uso y tratamiento de datos personales se fundamentará en lo establecido por la Ley y las demás disposiciones que la desarrollen.
- ✓ Principio de finalidad: La recolección, uso y tratamiento de datos personales obedecerán a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual será informada al titular de los datos.
- ✓ Principio de libertad: La recolección, uso y tratamiento de datos personales sólo puede ejercerse con el consentimiento previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin

previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

- ✓ Principio de veracidad o calidad: La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
- ✓ Principio de transparencia: En la recolección, uso y tratamiento de datos personales debe garantizarse el derecho del titular a obtener del responsable del tratamiento o del encargado, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.
- ✓ Principio de acceso y circulación restringida: La recolección, uso y tratamiento de datos sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la Ley y demás normas que la desarrollan.

Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a la ley.

- ✓ Principio de seguridad: Los datos personales e información sujeta a tratamiento público, será objeto de protección y deberá manejarse con las medidas y recursos técnicos, humanos y administrativos que sean necesarios para brindar seguridad a los registros, así como con la adopción de herramientas tecnológicas de protección, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- ✓ Principio de confidencialidad: Todas las personas que intervengan en la recolección, uso y tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, incluso luego de finalizada su relación con alguna de las labores que comprende el tratamiento.
- ✓ Principio de facilitación: Los responsables del tratamiento deberán facilitar el ejercicio del derecho de acceso a la información, excluyendo exigencias o requisitos que puedan obstruirlo o impedirlo.
- ✓ Principio de no discriminación: De acuerdo con el cual el responsable del tratamiento de datos deberá entregar información a todas las personas que lo soliciten, en igualdad de condiciones, sin hacer distinciones arbitrarias.
- ✓ Principio de gratuidad: Según el cual, el acceso a la información es gratuito y no se podrá cobrar valores adicionales al costo de reproducción de la información.

- ✓ Principio de celeridad: Este principio busca la agilidad en el trámite y la gestión administrativa.

Categorías Especiales de Datos

Datos 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 garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Tratamiento de datos sensibles:

Se prohíbe el tratamiento de datos sensibles, excepto cuando:

a.	El titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.
b.	El tratamiento sea necesario para salvaguardar el interés vital del titular y éste se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
c.	El tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de Ley, fundaciones, ONG, asociaciones o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del titular.
d.	El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

e.	El tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los titulares.

4.2 Derechos de los niños, niñas y adolescentes:

En la recolección, uso y tratamiento de los datos personales, se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes. Queda proscrito el tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública.

Es tarea del Estado y las entidades educativas de todo tipo de proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás.

5. Personas a Quienes se les Puede Suministrar la Información

La información y datos personales que reúnan las condiciones establecidas por la ley y las demás normas que la desarrollan, podrán suministrarse a las siguientes personas:

a.	A los titulares o sus representantes legales.
b.	A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.
c.	A los terceros autorizados por el titular o por la ley.

Excepciones de Acceso a la Información

El acceso a datos personales corresponde a una excepción de acceso a la información pública nacional, enmarcadas en el título III de la Ley 1712 de 2014.

- **Información exceptuada por daño de derechos a personas naturales o jurídicas:**

Hace alusión a toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito, siempre que el acceso pudiere causar daño a derechos como la intimidad, la vida, la salud y la seguridad.

Información exceptuada por daño a los intereses públicos:

Se refiere a aquella información pública reservada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito en las siguientes circunstancias, siempre que dicho acceso estuviere expresamente prohibido por una norma legal o constitucional.

- La defensa y seguridad nacional.
- La Seguridad pública.
- Las relaciones internacionales
- La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso.
- El debido proceso y la igualdad de las partes en los procesos judiciales.
- La administración efectiva de la justicia.
- Los derechos de la infancia y la adolescencia.
- La estabilidad macroeconómica y financiera del país.
- La Salud pública.
- En general toda afectación o amenaza que ponga en riesgo la seguridad del Estado o la de sus conciudadanos

- **Divulgación parcial:**

En aquellas circunstancias en que la totalidad de la información contenida en un documento no esté protegida por una excepción legal, deberá hacerse una versión publica que mantenga reserva únicamente de la parte indispensable, a efectos de garantizar el acceso a la información y al mismo tiempo, proteger debidamente los datos personales del titular.

DEBERES, AVISO DE PRIVACIDAD Y CRITERIO DIFERENCIA

- ✓ **Deberes de la Alcaldía de La Estrella como Responsable del Tratamiento de los Datos Personales**

La Alcaldía de La Estrella, actuando en calidad de responsable del tratamiento de datos personales, deberá:

a	Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
b	Solicitar y conservar copia de la respectiva autorización otorgada por el titular, para el uso y tratamiento de los datos personales.
c	Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten, en virtud de la autorización otorgada.
d	Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
e	Garantizar que la información que se suministre al encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
f	Actualizar la información, comunicando de forma oportuna al encargado del tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a éste, se mantenga actualizada.
g	Rectificar la información cuando sea incorrecta y comunicar lo pertinente al encargado del tratamiento.
h	Suministrar al encargado del tratamiento, según el caso, únicamente datos cuyo tratamiento esté previamente autorizado.
i	Exigir al encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular.
j	Tramitar las consultas y reclamos formulados.
k	Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y para la atención de consultas y

	reclamos.
l	Abstenerse de circular información que esté siendo controvertida por el titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
m	Registrar en la base de datos respectiva, la leyenda “reclamo en trámite” en la forma en que se regula en la presente Resolución.
n	Insertar en la base de datos la leyenda “información en discusión judicial” una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
o	Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella o a quien ostente la debida autorización en forma idónea o legal.
p	Informar a solicitud del titular sobre el uso dado a sus datos, finalidad de la recolección y los derechos vinculados a éste, procedentes desde la autorización otorgada.
q	Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.
r	Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

- ✓ **Aviso de Privacidad**

Cuando no sea posible poner a disposición del titular de los datos personales la Política de Tratamiento de la Información, la Alcaldía de La Estrella informará por medio de un Aviso de Privacidad, sobre la existencia de tales políticas.

El Aviso de Privacidad se expedirá en medios físicos, electrónicos o en cualquier otro formato, en donde se ponga a disposición del titular de los datos, además de la existencia de políticas de tratamiento de datos, la forma de acceder a ellas y la finalidad que se pretende dar a la información; el aviso se enviará al correo electrónico o dirección física cuando se disponga de dicha información. En caso

contrario, se publicará en la página web de la entidad en documento dirigido al titular de los datos.

Contenido del Aviso de Privacidad

1	Nombre o razón social y datos de contacto del responsable del tratamiento.
2.	El tratamiento al cual serán sometidos los datos y la finalidad del mismo.
3.	Los derechos que le asisten al titular.
4.	Los mecanismos dispuestos por la Entidad para que el titular conozca la Política para el Tratamiento de Datos Personales y los cambios sustanciales que se produzcan en ella o en el Aviso de Privacidad.
5.	Información sobre consulta y acceso a la Política para el Tratamiento de Datos Personales.

Cuando se trate de la recolección de datos personales sensibles, el Aviso de Privacidad deberá señalar expresamente el carácter facultativo para atender las preguntas relacionadas con este tipo de datos.

- ✓ **Criterio Diferencial de Accesibilidad**

Con el objeto de facilitar que las poblaciones especificas accedan a la información que particularmente las afecte, los sujetos responsables del tratamiento, divulgarán la información pertinente en diversos idiomas y lenguas y, a su vez, elaborarán formatos alternativos comprensibles para grupos diferenciales, asegurando el acceso a esa información a los distintos grupos étnicos y culturales del país, así como a la adecuación de los medios de comunicación, para facilitar y garantizar el acceso a personas en situación de discapacidad.

POLÍTICA PARA EL TRATAMIENTO DE DATOS PERSONALES

1. Función de Protección de Datos Personales

La Alcaldía de La Estrella como Entidad pública actuará como responsable del tratamiento de los datos personales y hará uso de estos únicamente para las finalidades para las que se encuentra facultado, especialmente las señaladas en el título “Modo en que se utiliza la información” de la presente política y sobre la base de la ley y la normatividad vigente.

Datos de identificación del responsable del tratamiento:

Nombre: Alcaldía de La Estrella

Dirección: Calle 80 sur N°. 58 78 La Estrella-Antioquia

PBX: (57+4) 5407444

Línea Gratuita de atención al cliente: 018000420080

Correo: contactenos@laestrella.gov.co

Portal Web: www.laestrella.gov.co

Canales de servicio:

Escrito: Calle 80 sur No. 58 78 (oficina de archivo piso 1 del CAM), La Estrella-Antioquia

Correo electrónico: contactenos@laestrella.gov.co

Formulario PQR ubicado en el portal www.laestrella.gov.co, link; http://pqrs.laestrella.gov.co/

Presencial

Calle 80 sur No. 58 78 (oficina de archivo piso 1 del CAM), La Estrella-Antioquia

Telefónico

Conmutador 5407444

Virtual (Chat general o temático), sitio web www.laestrella.gov.co

2. **Información que se Recopila**

La Alcaldía de La Estrella recolecta información y datos personales en el momento en que son ingresados en el sistema de peticiones, quejas, reclamos, sugerencias, felicitaciones, consultas y denuncias por actos de corrupción, en las cuales el titular informa libremente sus datos personales, principalmente los relacionados con su nombre, tipo y número de documento de identidad, dirección de domicilio, dirección de correo electrónico, número telefónico de contacto, entre otros.

Adicionalmente, la Alcaldía de La Estrella administra los datos registrados a través del Sistema de Información y Gestión del Empleo Público –SIGEP, el cual contiene información de carácter institucional, como las hojas de vida y la declaración de bienes y rentas de servidores públicos y contratistas del Estado.

Finalmente se recolecta y administran los datos personales de los ciudadanos encuestados, como parte de los procesos de medición de satisfacción que adelante la entidad.

La Alcaldía de La Estrella podrá solicitar información adicional (sensible), la cual podrá ser suministrada por parte del titular de manera libre y voluntaria.

3. **Modo en que se Utiliza la Información**

Previa autorización del titular de los datos personales, le permitirá a la Alcaldía de La Estrella darle el siguiente tratamiento:

- ✓ Para los fines administrativos propios de la Entidad.
- ✓ Caracterizar ciudadanos y grupos de interés y adelantar estrategias de mejoramiento en la prestación del servicio.
- ✓ Dar tratamiento y respuesta a las peticiones, quejas, reclamos, denuncias, sugerencias y/o felicitaciones presentados a la Entidad.
- ✓ Alimentar Sistemas de Información.
- ✓ Conocer y consultar la información del titular del dato que reposen en bases de datos de entidades públicas o privadas.
- ✓ Adelantar encuestas de satisfacción de usuarios.
- ✓ Envío de información de interés general.
- ✓ Recopilar información de ciudadanos asistentes a capacitación desarrolladas por la Entidad.

La información y datos personales suministrados por el titular de los mismos, podrán ser utilizados por la Alcaldía de La Estrella como responsable del tratamiento de los datos, para el desarrollo de las funciones propias de la entidad. Cualquier otro tipo de finalidad que se pretenda dar a los datos personales, deberá ser informado previamente, en el aviso de privacidad y en la respectiva

autorización otorgada por el titular del dato, según sea el caso, y siempre teniendo en cuenta los principios rectores para el tratamiento de los datos personales, establecidos por la Ley, el presente documento y las demás normas que desarrollen la materia.

Derechos de los Titulares de los Datos Personales

La Alcaldía de La Estrella, garantiza al titular de datos personales, el pleno ejercicio de los derechos que se enlistan a continuación:

- ✓ Conocer, actualizar y rectificar sus datos personales. Este derecho se podrá ejercer también, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
- ✓ Solicitar prueba de la autorización otorgada la Alcaldía de La Estrella para el tratamiento de sus datos personales.
- ✓ Ser informado del uso y tratamiento dado a sus datos personales, previa solicitud elevada a través de los canales de servicio.
- ✓ Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la ley y las demás normas que la modifiquen, adicionen o complementen.
- ✓ Revocar la autorización y/o solicitar la supresión de uno a más datos cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el tratamiento de los datos se ha incurrido en conductas contrarias a la ley y a la Constitución.
- ✓ Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

Autorización

La Alcaldía de La Estrella solicitará a más tardar en la recolección de la información, autorización del titular para el uso y tratamiento de sus datos personales, salvo en los casos exceptuados por la ley; dicha autorización deberá estar contenida en un documento físico o electrónico.

Autorización para el Tratamiento de datos personales sensibles

La recolección, uso y tratamiento de datos sensibles (aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación ej. origen racial, religión, adscripción ideológica, etc.) está prohibido, a excepción de los casos señalados por la ley; cuando el tratamiento sea posible, se deberá:

Informar al titular que por tratarse de datos sensibles no está obligado a autorizar su tratamiento.

Informar al titular previamente y de forma explícita, los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, los datos sensibles que serán objeto de tratamiento, y la finalidad del tratamiento, así como obtener del titular su consentimiento expreso.

Revocatoria de la autorización

El titular de los datos personales podrá en todo momento solicitar a la Alcaldía de La Estrella la revocatoria de la autorización otorgada, mediante la presentación de un reclamo. La revocatoria de la autorización no procederá cuando el titular tenga un deber legal o contractual de permanecer en la(s) base(s) de datos de la Entidad.

Si vencido el término legal para atender el reclamo, la Alcaldía de La Estrella no ha eliminado los datos personales, el titular tendrá derecho a solicitar a la Superintendencia de Industria y Comercio que ordene la revocatoria de la autorización.

Procedimiento para Consultas

Los titulares, sus causahabientes o representantes podrán consultar la información personal del titular que repose en cualquier base de datos, por lo que la Alcaldía de La Estrella como responsable del tratamiento, suministrará a éstos, toda la información contenida en el registro individual o que esté vinculada con la identificación del titular.

Para lo anterior, será necesario acreditar con el documento de identificación pertinente, la calidad de titular o causahabiente

La Alcaldía de La Estrella brindara los medios de comunicación electrónica para la formulación de consultas, los cuales serán los mismos utilizados para la recepción y atención de peticiones, quejas, reclamos, sugerencias, denuncias y/o felicitaciones.}

La solicitud para realizar consultas de datos personales debe ser radicada o presentada en medio físico en la siguiente dirección:

Calle 80 sur No. 58 78 Centro Administrativo Jorge Eliecer Echavarria Henao (La Estrella-Antioquia) - piso 1, oficina de archivo municipal.

Medio electrónico:

Sitio web www.laestrella.gov.co, link peticiones , quejas y reclamos http://pqrs.laestrella.gov.co/

Teniendo en cuenta los términos establecidos por la normatividad vigente, La Alcaldía de La estrella informa que la consulta será atendida en un término máximo de diez (10) días hábiles, contados a partir de la fecha de recibo de la misma. De cumplirse el término sin que sea posible atender la consulta, la Alcaldía de La Estrella como responsable del tratamiento de los datos, informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual no podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

Procedimiento para Reclamos

Los titulares o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la Ley y demás normas que la desarrollan, podrán presentar un reclamo que será tramitado bajo las siguientes reglas:

Contenido:

- Identificación del titular del dato.
- Descripción precisa de los hechos que dan lugar al reclamo.
- Datos de notificación, dirección física y/o electrónica.
- Los demás documentos que se quiera hacer valer.

Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga “reclamo en trámite” y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

El reclamo será atendido en quince (15) días hábiles como máximo, contados a partir del día siguiente a la fecha de su recibo. Si no fuere posible atender el reclamo dentro del término establecido, la Alcaldía de La Estrella informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, el cual no podrá superar a ocho (8) días hábiles siguientes al vencimiento del primer término.

Derecho de Acceso a los Datos

La Alcaldía de La Estrella garantiza el derecho de acceso a los datos personales, una vez se haya verificado la identidad del titular, su causahabiente y/o representante, poniendo a disposición de éste, los respectivos datos personales.

Para tal efecto se brindará los medios de comunicación y mecanismos electrónicos y/o presenciales sencillos y con disponibilidad permanente, los cuales permitan el acceso directo del titular a los datos personales, los cuales serán informados en el Aviso de Privacidad o en el Formato de Autorización para el tratamiento de datos personales.

Procedimiento Actualización y Rectificación de Datos

La Alcaldía de La Estrella, como responsable del tratamiento de los datos, deberá rectificar y actualizar a solicitud del titular toda información que de éste resulte ser incompleta o inexacta. Para estos efectos, el titular o su causahabiente y/o representante, señalará las actualizaciones y rectificaciones a que dieran lugar, junto a la documentación que soporte su solicitud.

La Alcaldía de La Estrella habilitará los medios físico Calle 80 sur N°. 58 78 Centro Administrativo Jorge Eliecer Echavarria Henao (La Estrella-Antioquia) - piso 1, oficina de archivo municipal y electrónicos existentes en la Entidad encaminados a garantizar este derecho, que serán los mismos utilizados para la recepción y atención de peticiones, quejas, reclamos, sugerencias, denuncias y/o felicitaciones administrado por la secretaria general de la entidad.

Supresión de Datos

Los Titulares podrán en todo momento y cuando consideren que los datos no están recibiendo un tratamiento adecuado o los mismos no son pertinentes o necesarios para la finalidad para la cual fueron recolectados, pueden solicitar a la Alcaldía de La Estrella la supresión de sus datos personales mediante la presentación de un reclamo.

No obstante, la solicitud de supresión de datos no procederá cuando el titular tenga un deber legal o contractual de permanecer en la(s) base(s) de datos o la

supresión de los datos represente un impedimento en actuaciones administrativas o judiciales relacionadas a obligaciones fiscales, investigación de delitos o actualización de sanciones administrativas.

Si vencido el término legal respectivo, no se han eliminado los datos personales, el titular tendrá derecho a solicitar a la Superintendencia de Industria y Comercio que ordene la supresión de los datos personales.

La Alcaldía de La Estrella brindara los medios de comunicación electrónica u otros para solicitud de supresión de datos, que serán los mismos utilizados para la recepción y atención de peticiones, quejas, reclamos, sugerencias, denuncias y/o felicitaciones administrado por la secretaria general de la entidad.

11. **Persona o grupo responsable de la Atención de Peticiones, Consultas, Reclamos y Denuncias**

El Área encargada de atender las Quejas, Reclamos, Consultas y Denuncias sobre el tratamiento de datos personales es la Secretaria General de la Alcaldía de La Estrella, ubicado en la Calle 80 sur No. 58 78 Centro Administrativo Jorge Eliecer Echavarría Henao (La Estrella-Antioquia) - piso 8, secretaria general, horario de atención de lunes a jueves de 7:30 am a 12:30 pm y de 1:30 pm a 5:30 pm, los viernes de 7:30 am a 12:30 am y de 1:30 pm a 4:30 pm, en el teléfono 5407444 o vía correo electrónico en contectenos@laestrella.gov.co.

12. Seguridad de la Información

La Alcaldía de La Estrella brindara el uso de medidas técnicas, humanas, administrativas y electrónicas necesarias para otorgar seguridad a los datos personales y demás información sujeta a tratamiento, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

13. Vigencia y Aviso de Posible Cambio Sustancial en las Políticas de Tratamiento

La presente Política para el Tratamiento de Datos Personales rige a partir de la expedición y publicación del manual y la Resolución que la reglamenta, se divulgará a través del portal institucional, y estará sujeto a actualizaciones en la medida en que se modifiquen o se dicten nuevas disposiciones legales sobre la materia.

Cuando se cumplan estas condiciones, la Alcaldía de La Estrella informará a los titulares de los datos personales, sus causahabientes o representantes, las nuevas medidas dictadas sobre la materia, antes de implementar las nuevas

políticas. Además, deberá obtener del titular una nueva autorización cuando el cambio se refiera a la finalidad del tratamiento.

BIBLIOGRAFIA

Departamento Administrativo de la Función Pública, Instructivo de la Política para el Tratamiento de Datos Personales, https://www.funcionpublica.gov.co/documents/418537/1512450/InstructivoPolitica_Datos.pdf/f7d7cbe2-6739-46de-9f76-ee147cf1aa60

Modelo de Seguridad - Fortalecimiento TI – MinTIC, https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

Modelo Integrado de Planeación y Gestión, en donde encontrará la información necesaria para implementar MIPG en las entidades públicas, https://www.funcionpublica.gov.co/web/mipg.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL SITIO WEB

1. Sobre las bases de datos y archivos almacenados:

   Toda la información publicada en el sitio web se encuentra almacenada en una base de datos y un sistema de archivos que cuenta con un nivel alto de seguridad y restricción de usuarios con el fin de garantizar la integridad y veracidad de la información que allí se publica.

2. Sobre las copias de seguridad:

   Se implementó un mecanismo que diariamente realiza una copia completa de la base de datos y el sistema de archivos para mitigar cualquier tipo de vulneración o pérdida de información.

3. Sobre el certificado de seguridad y sesiones seguras:

   El sitio web cuenta con un certificado de seguridad (SSL) el cual garantiza que la información presentada, lo es de manera segura y verificada ante el proveedor de internet por el cual el usuario se está conectado al sitio web. De igual forma se recomienda a los visitantes del sitio web ingresar por medio del dominio seguro http://laestrella.gov.co y evitar ingresar por medio de vínculos en páginas no verificadas.

4. Sobre los registros de auditoría:

   El sitio web cuenta con un mecanismo de auditoria que contiene toda la información que es ingresada, modificada o eliminada del sitio web, los usuarios pueden encontrar estos registros de auditoría dentro de la sección de Transparencia, en el menú, Instrumentos de Gestión Pública y en el ítem Registro de Publicaciones. O en el siguiente enlace: http://laestrella.gov.co/alcaldia/registro_publicaciones.

POLÍTICA DE PRIVACIDAD Y CONDICIONES DE USO DEL SITIO

1. Sobre los enlaces:

   El sitio web contiene enlace a sitios externos de los cuales no se tiene ningún control alguno, por esta razón no se hace responsable por la información allí contenida.

2. Sobre el soporte técnico:

Para cualquier inquietud, comentario, sugerencia o solicitud respecto al contenido del sitio web deberá ser notificada por medio del formulario de contáctenos que se encuentra en el menú atención al ciudadano, en el ítem formulario de contáctenos. De igual manera se puede enviar un correo electrónico a contactenos@laestrella.gov.co

3. Sobre confidencialidad de la información:

   La entidad no compartirá, ni revelará la información confidencial con terceros que haya sido suministrada por medio de los formularios del sitio web, excepto que tenga expresa autorización de quienes se suscribieron, o cuando ha sido requerido por orden judicial o legal, o para proteger los derechos de propiedad intelectual u otros derechos del sitio Web.

El presente manual de Políticas específicas de seguridad de la información se presentó en mesa de trabajo al Comité Municipal de Gestión y Desempeño del Municipio de La Estrella, en donde mediante Acta 001 del 15 de agosto de 2019 se aprueba y se envía revisión final y jurídica para elevar la aprobación mediante Decreto firmado por el señor Acalde.

Instancia de Aprobación: Comité Municipal de Gestión y Desempeño del Municipio de La Estrella

Nombre	Cargo	Firma
JHONNY ALEXANDER GARCIA YEPES	Alcalde Municipal / Presidente	
CLAUDIA URIBE TOBON	Secretaria General	
MARTA LUZ MESA	Secretaria de la Mujer	
SANDRA MILENA MEJIA	Secretaria de Control Interno	
JHONATAN LUNDER FLOREZ	Secretario de Educación	
ANA MARIA RIOS RESTREPO	Secretaria de Obras Publicas	
ALEJANDRO ESCOBAR C.	Secretario de Transito	
PILAR ASTRID POSADA JIMENEZ	Secretaria de Servicios Administrativos	
DIANA CAROLINA FERNANDEZ	Secretaria de Gobierno	

HECTOR MARIO CANO	Secretario de Hacienda	
JUAN GREGORIO FERNANDEZ GALLEGO	Secretario de Planeación / Quien hace las veces de Secretario Técnico del Comité	
JOSE DANIEL GOMEZ	Gerente Promotora Proyectos Siderenses	

Elaborado Por:

Nombre	Cargo	Firma
ALEJANDRO BAENA CUARTAS	CONTRATISTA SERVICIOS ADMINISTRATIVOS	

DOCUMENTO QUE APRUEBA:

Tipo De Documento	Numero	Fecha
ACTA DE REUNION ORDINARIA	Acta 001	15 de Agosto de 2019