Alcaldía Distrital de Buenaventura

NUESTRA RIQUEZA NOS VIENE DEL MAR

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

OFICINA TIC

ALCALDÍA DISTRITAL DE BUENAVENTURA 2022

	ALCALDÍA DISTRITAL DE BUENAVENTURA PROCESO: PROCESO: PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	

TABLA DE CONTENIDO

	ALCALDÍA DISTRITAL DE BUENAVENTURA PROCESO: PROCESO: PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	

CONTROL DE CAMBIOS		
Versión	**Fecha**	**Descripción**
2022-01	28-01-2022	Se actualizó la Normatividad relacionada con la política de privacidad de la información.

INTRODUCCIÓN

La Alcaldía Distrital de Buenaventura con el propósito de salvaguardar la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha establecido realizar un Plan de Seguridad y Privacidad de la información con el ánimo de que no se presenten pérdidas, robos, accesos no autorizados y duplicación de la misma, igualmente promueve una política de seguridad de la información física y digital de acuerdo a la caracterización de los usuarios tanto internos como externos.

En concordancia con el decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la Política de Gobierno Digital (antes estrategia de Gobierno en Línea GEL) y siguiendo las directrices del Marco de Referencia de Arquitectura Empresarial para la Gestión T.I. del Estado colombiano, el Plan de Seguridad y Privacidad de la información PSPI en su versión 02, se convertirá en una herramienta fundamental para la toma de decisiones en la Administración Distrital de Buenaventura.

El presente plan se concibe para ser modificado periódicamente; ajustándose a los cambios que se vayan suscitando con relación a la ley de Transparencia y Acceso a la Información Pública, legislación de la Ley de Protección de Datos Personales y demás normas concomitantes.

OBJETIVOS

Objetivo General

- Establecer las políticas para garantizar la administración, manejo y control de la seguridad y privacidad de la información de la Alcaldía de Distrital de Buenaventura.

Objetivos Específicos

- Establecer políticas de seguridad y privacidad de la información de la Alcaldía Distrital de Buenaventura.
- Optimizar la gestión de la seguridad de la información al interior de la Administración Distrital, sus entidades descentralizadas y demás.
- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Contribuir a mejorar los procesos de intercambio de información pública.
- Definir el alcance de las políticas de Seguridad y Privacidad de la Información.
- Contribuir en el desarrollo del ejercicio de arquitectura empresarial apoyando en el cumplimiento de los lineamientos del marco de referencia de arquitectura empresarial para la gestión de TI del estado colombiano.

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Alcaldía del Distrito de Buenaventura considera la información como un bien público de vital

importancia para el cumplimiento de su función pública y normal desempeño, por lo tanto, es compromiso de la alta dirección de la entidad el establecimiento, implementación, mantenimiento y mejora de la seguridad y privacidad de la información con el objetivo de minimizar los riesgos internos o externos, deliberados o accidentales de acceso a la información y apoyar el cumplimiento de los objetivos estratégicos y adecuada al propósito de la entidad.

La seguridad y privacidad de la información se entiende como la preservación de las siguientes características:

Confidencialidad: es un conjunto de reglas que limita el acceso a la información.

Integridad: es la garantía de que la información es confiable y precisa.

Disponibilidad: es una garantía de acceso confiable a la información por parte de personas autorizadas.

La Alcaldía del Distrito de Buenaventura en su propósito de dar cumplimiento con la política establecida de seguridad y privacidad de la información establece los siguientes objetivos:

- Gestionar de manera eficaz los riesgos de seguridad y privacidad de la información identificados en la Entidad.
- Sensibilizar y apropiar la gestión adecuada de seguridad y privacidad de la información de los colaboradores, contratistas, terceros y demás partes interesadas de la entidad.
- Cumplir con las políticas, procedimientos e instructivos de Seguridad de la Información.

Alcance/Aplicabilidad

Esta política aplica a toda la entidad, servidores públicos, contratistas y terceros de la Alcaldía del Distrito de Buenaventura.

Cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento con la presente política.

El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la entidad, incluyendo lo establecido en las normas que competen al gobierno nacional y territorial en cuanto a seguridad y privacidad de la información se refiere.

Normatividad

A continuación, se referencian las normas y leyes colombianas que aplican en el ámbito de seguridad de la información, si cualquier disposición de estas condiciones pierde validez o fuerza obligatoria, por cualquier razón, todas las demás disposiciones conservan su fuerza obligatoria y carácter vinculante.

- Constitución Política de Colombia Artículo 15. “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacer los respetar”. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
- Constitución Política de Colombia Articulo 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios de comunicación masiva. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.
- Ley 23 de 1982, Sobre derechos de autor
- Ley 527 de 1999, Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos.
- Ley 594 de 2000, Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones.
- Ley 603 de 2000, Por la cual se modifica el artículo 47 de la Ley 222 de 1995,
- Articulo 2. Artículo 2º. Las autoridades tributarias colombianas podrán verificar el estado de cumplimiento de las normas sobre derechos de autor por parte de las sociedades para impedir que, a través de su violación, también se evadan tributos.
- Decreto 1747 de 2000, por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.
- Ley 679 de 2001, Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución.
- Ley 734 de 2002, Por medio de la cual se expide del código único disciplinario.
- Ley 1032 de 2006, Por la cual se modifican los artículos 257, 271, 272 y 306 del Código Penal. Artículo 271. Violación a los derechos patrimoniales de autor y derechos conexos. Modificación del código Penal Colombiano Ley 599 de 2000.
- Ley 1266 de 2008, Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de

terceros países.

- Ley 1221 de 2008, Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- Ley 1341 de 2009, Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC.
- Ley 1273 de 2009, Por medio de la cual se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.
- Ley 1336 de 2009 (Lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes.) por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes.
- Ley 1437 DE 2011, por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo. (Uso de medios electrónicos Procedimiento Administrativo Electrónico), Articulo 1 de la ley 1755 de 2015.
- LEY 1474 DE 2011 Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- Ley 1581 de 2012, Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales.
- Ley 1672 de 2013, Lineamientos para la Adopción de una política pública de gestión integral de residuos de aparatos eléctricos y electrónicos.
- 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.
- Ley 128 de 2018, Por medio de la cual se aprueba el “Convenio sobre la Ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest.
- Ley 1955 del 25 de mayo de 2019. “Por el cual se expide el Plan Nacional de Desarrollo 2018- 2022. “Pacto por Colombia, Pacto por la Equidad”. Incluyó el artículo 147 de Transformación Digital Pública y 148 de Gobierno Digital como política de gestión y desempeño institucional
- Decreto 1474 de 2002, por el cual se promulga el “Tratado de la OMPI, Organización Mundial de la Propiedad Intelectual, sobre Derechos de Autor (WCT)”, adoptado en Ginebra, el veinte (20) de diciembre de mil novecientos noventa y seis (1996).
- Decreto 4632 de 2011 Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.
- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del

Estado".

- Decreto 103 de 2015, Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
- Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo
- Decreto 1081 de 2015 (Decreto Reglamentario Único del Sector Presidencia de la Republica), Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República, Título 1, Disposiciones generales en materia de transparencia y del derecho de acceso a la información pública nacional
- Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública
- Decreto 1494 de 2015, Por el cual se corrigen yerros en la Ley 1712 de 2014
- 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
- Decreto No. 2106 del 22 de noviembre de 2019. “Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.”
- Documento CONPES 3854, Política Nacional de Seguridad Digital
- Documento CONPES 3975, Política Nacional para la Transformación Digital e Inteligencia Artificial, del 8 de noviembre de 2019. El Consejo Nacional de Política Económica y social (CONPES)
- Directiva Presidencial 02 del 2 de abril de 2019. Simplificación de la interacción digital los ciudadanos y el Estado.
- Circular Externa Conjunta No. 04 del 5 de septiembre de 2019. Tratamiento de datos personales en sistemas de información interoperables.
- Norma Técnica Colombiana NTC- ISO/IEC Colombiana 27001:2013. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Justificación

La Alcaldía Distrital de Buenaventura considera la información como un bien público de vital importancia para el cumplimiento de su función pública y normal desempeño, con el fin de preservar, proteger, administrar y gestionar esta información se ha establecido realizar un Plan de Seguridad y Privacidad de la información con el objetivo de minimizar los riesgos internos o externos, deliberados o accidentales de acceso a la información.

La seguridad de la información se entiende como la preservación de las siguientes características:

- Confidencialidad: es un conjunto de reglas que limita el acceso a la información.
- Integridad: es la garantía de que la información es confiable y precisa.
- Disponibilidad: es una garantía de acceso confiable a la información por parte de personas autorizadas.

Objetivo de la Implementación de la Política

Definir los mecanismos para el manejo que tienen los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad, con el propósito de mitigar el riesgo de acceso, uso, divulgación, interrupción o destrucción no autorizada de la misma. Asegurando el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Alcance

Este documento da los lineamientos requeridos para normalizar la seguridad y privacidad de la información y seguridad digital en la Alcaldía Distrital de Buenaventura, se aplica a todos los funcionarios, contratistas y terceros, así como a los procesos y procedimientos, que manejen activos de información de la entidad.

Roles y Responsabilidades

El Comité de Seguridad de la Información es el máximo órgano al que compete la Seguridad de la Información en la organización. Es responsabilidad de este la implementación, aplicación, seguimiento y autorizaciones de la política del Plan de Seguridad y Privacidad de la información en las diferentes áreas y procesos de la entidad, además garantiza el apoyo y el uso de la Política de Seguridad de la Información como parte de su herramienta de gestión, la cual debe ser aplicada de forma obligatoria por todos los funcionarios para el cumplimiento de los objetivos. En este sentido, define las estrategias relacionadas con la seguridad de la información.

El Comité de Seguridad de la Información estará conformado por:

- Secretario General.
- El Coordinador de Sistemas o responsable del área TIC.
- El Jefe de Control Interno.
- El Jefe de Planeación.
- El secretario de Hacienda.
- Jefe Departamento Jurídico.

Es el comité el encargado de revisar anualmente que estas políticas aquí detalladas se cumplan.

Cumplimiento

Las políticas de seguridad y privacidad de la información son obligatorias para todos los funcionarios de la administración y/o entes externos a la alcaldía y el no cumplimiento es considerado una violación grave por lo cual la alcaldía de Buenaventura está en el derecho de tomar las medidas sancionatorias que correspondan.

Comunicación

Por medio de documento escrito y otros medios digitales como sitio Web y correo electrónico, se debe dar a conocer a todos los funcionarios de la alcaldía el contenido de las políticas de seguridad y privacidad de la alcaldía a funcionarios, contratistas y/o terceros, para que estos conozcan sus disposiciones, efectos y retroalimenten las mismas con fines que todos puedan cumplirlas dentro del plan.

Monitoreo

Se debe crear un mecanismo de medición, con sus correspondientes indicadores relacionados con las políticas de seguridad y privacidad de la información, con el fin de determinar el cumplimiento de las mismas y/o para establecer qué modificaciones o adiciones se deben efectuar, con base en las evaluaciones, seguimiento y control realizado por la Oficina de Control Interno.

DESCRIPCIÓN DE LAS POLÍTICAS

En la alcaldía de Buenaventura cada una de sus áreas maneja un número de procesos los cuales cuentan con una correspondiente información, que en algunos casos es clasificada y/o reservada, es sobre ésta que toda la entidad lleva a cabo su funcionamiento por lo tanto se deben crear criterios para su manipulación.

Todos los mecanismos determinados para su manejo deben estar considerados sobre los criterios de integridad, disponibilidad y confidencialidad.

Luego de determinar las políticas, los objetivos y el alcance de los sistemas de seguridad de la información de la entidad, se divulga la misma y se definen los controles de seguridad requeridos con el fin de mantener y gestionar el riesgo como lo establece la política de los riesgos institucionales. El objeto de la documentación y elaboración de las políticas de seguridad y prevención de la información busca que se pueda mantener y gestionar de manera dinámica el riesgo institucional y la continuidad del negocio.

POLÍTICAS

Políticas de dispositivos móviles

- ✔ La Entidad establece las condiciones para el uso seguro de los dispositivos móviles (portátiles, teléfonos, inteligentes, tabletas, entre otros) institucionales que hagan uso de servicios de la Entidad como son: Establecer contraseñas de acceso robustas, cifrar la información almacenada, mantener el dispositivo móvil con el sistema operativo siempre actualizado y con un antivirus activo.

- ✔ Si los funcionarios o contratistas hacen uso de aplicaciones móviles con información de la entidad en sus dispositivos personales, se deben tener en cuenta las condiciones descritas en el ítem anterior.

- ✔ Los funcionarios y contratistas no están autorizados a cambiar la configuración, ni la instalación/desinstalación de las aplicaciones móviles de los dispositivos móviles institucionales que se les entregue como recurso para la ejecución de sus obligaciones o funciones.

- ✔ Es responsabilidad del servidor público al que se le asignó el dispositivo móvil evitar la instalación de programas desde fuentes desconocidas, evitar el uso de redes inalámbricas públicas, y mantener desactivadas las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.

Políticas teletrabajo

- ✔ Toda información gestionada por la Entidad, y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales con esta.

- ✔ La Entidad establece los requerimientos para autorizar conexiones remotas a la infraestructura tecnológica necesaria para la ejecución de las funciones de los servidores públicos y contratistas de la entidad, garantizando las herramientas y controles para proteger la confidencialidad, integridad y disponibilidad de las conexiones remotas.

- ✔ La Entidad establece el proceso de implementación de teletrabajo, de acuerdo con la normativa y los lineamientos exigidos, con el fin de proteger la información.

Políticas de seguridad de los recursos humanos

- ✔ El área que realice la contratación de personal en la Entidad realiza las verificaciones de los antecedentes (procuraduría, contraloría, policía) de los candidatos al cargo, la formación académica, experiencia y demás información que se requiera, de acuerdo con las leyes, reglamentos de la Entidad y ética pertinente.

- ✔ Todo servidor público y contratista debe recibir inducción y procesos periódicos de sensibilización en seguridad y privacidad de la información en la Entidad

- ✔ La Entidad debe incorporar los roles y responsabilidades en seguridad de la información dentro de las funciones y obligaciones contractuales de los Colaboradores y Terceros.

Políticas gestión de activos

- ✔ La Entidad establece los métodos de identificación, clasificación y valoración de activos de información, así como la definición de la asignación de responsabilidades, manteniendo mecanismos acordes para el control de riesgos de la información.

- ✔ Los servidores públicos y contratistas deben hacer la devolución de los activos de información asignados a su cargo una vez finalice la relación contractual con la Entidad.

- ✔ Los equipos portátiles o Todo en uno deben contar con guaya de seguridad para evitar su robo.

- ✔ No se puede retirar ningún equipo de cómputo, ni servidor, ni equipo de telefonía IP de la Entidad sin haber diligenciado el formato de salida de estos elementos, el cual debe estar autorizado por el jefe del área y el jefe de servicios Básicos.

- ✔ La Entidad debe contar con un sistema o listado de equipos de cómputo portátil asignado a funcionarios o contratistas para validar la salida de los mismos sin la necesidad del formato de salida de elementos.

- ✔ Todo equipo de computo que ingrese a la entidad, debe ser reportado en la entrada mediante formato de registro, donde se identifique: marca, serial, tipo, propietario, fecha y hora de entra, fecha y hora de salida del mismo.

- ✔ Es responsabilidad del líder de proceso, jefe de área o director, la identificación y reporte de nuevos activos de información, así mismo mantener actualizada la valoración de estos.

Políticas gestión de medios de almacenamiento

- ✔ Todo medio removible en estado de tránsito o préstamo deberá ser autorizado por el propietario del activo de información.

- ✔ Todo proceso para para dar de baja o reutilización de dispositivos que contengan información almacenada, se debe proceder con la destrucción o borrado seguro.

- ✔ Cada medio removible de almacenamiento se identificará de acuerdo a la información contenida.

Políticas control de acceso y Manejo de la Información

- ✔ La Entidad establece procedimientos para la creación de datos de acceso, suministro de accesos a la información, revisión periódica de los accesos otorgados, y desactivación o eliminación de las cuentas de usuario una vez finalizada la relación contractual.

- ✔ Todos los usuarios en su primer inicio de sesión deben cambiar las contraseñas suministradas de acceso a la red, sistemas de información, aplicaciones, entre otros.

- ✔ Todos los usuarios de sistemas de información deberán cambiar sus contraseñas de manera periódica. Las contraseñas son personales e intransferibles, y todo lo que ocurra en un sistema de información con determinado usuario, será responsabilidad de éste.

- ✔ Todos los servidores públicos y contratistas con acceso a un sistema de información o a la red informática institucional, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña y serán responsables de las acciones realizadas por el usuario que les ha sido asignado.

- ✔ Toda información institucional, debe manejarse a través de los correos electrónicos institucionales, el cual debe ser accedido desde equipos o dispositivos seguros.

- ✔ El acceso a Aplicativos Web de la entidad alojados en la nube, debe hacer desde equipos o dispositivos que briden las garantías suficientes de seguridad y responsabilidad del usuario, cualquier violación a la política de seguridad.

Políticas seguridad física y del entorno

- ✔ Los equipos de cómputo que pasen a un estado de retiro o se requieran para la reutilización deberán cumplir los siguientes lineamientos: a. Al momento de retirar un equipo en la organización (almacén), el proceso de TI realiza una copia de respaldo de la información almacenada en este activo. b. El proceso de TI realiza el proceso de borrado seguro de la información almacenada en los equipos que van a ser cedidos o utilizados en la organización.

- ✔ Para todos los usuarios de las aplicaciones y sistemas de información de la Entidad, es obligatorio que las sesiones sean cerradas al finalizar las actividades y no se deben dejar abiertas o desatendidas.

- ✔ Las áreas dentro de las cuales se encuentran el Centro de Datos, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, deben contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la información.

Política de controles criptográficos

- ✔ Los discos duros internos, externos y memorias USB utilizados por las diferentes áreas o procesos de la Entidad, están cifrados mediante algoritmos de cifrado simétrico. El personal de cada proceso es quien debe solicitar el cifrado de la información que esté clasificada como crítica o sensible por la Entidad.

- ✔ La Entidad asegura el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la integridad y el no repudio de la información. Por lo cual establece técnicas criptográficas y cifrado como son: Cifrado de la información cuando se requiere transferir o almacenar información sensible o crítica, uso de protocolos seguros para las redes Wifi, uso de protocolo HTTPS con un nivel de cifrado actualizado.

- ✔ El acceso remoto a la red y los sistemas de información de la Entidad desde una red externa será a través de conexiones seguras.

Políticas seguridad en las operaciones

- ✔ La Entidad documenta los procesos operacionales a nivel de TI, para reducir riesgos asociados con ausencia de personal y afectaciones en la infraestructura tecnológica.

- ✔ La Entidad garantiza que las operaciones Tecnológicas se gesten de forma correctas y se brinde seguridad a las instalaciones de procesamiento de información.

- ✔ Los cambios en la Entidad deben ser tratados a través de un proceso establecido con el fin de minimizar los riesgos de alteración de los sistemas de información.

- ✔ Según la clasificación de la información establecida por la Entidad, se establecen las medidas de respaldo de la información a través de mecanismos como cintas, discos de almacenamiento o en la nube.

Políticas seguridad de las comunicaciones

- ✔ El Proceso de TI realiza el bloqueo a las páginas de contenido para adultos, mensajería instantánea y demás páginas que no sean de uso institucional, mediante el uso de servidor proxy, firewall o control que mejor se ajuste a la necesidad.

- ✔ La Entidad asegura la protección de las redes y la transferencia de información. Para dar cumplimiento se deben firmar acuerdos de confidencialidad y de no divulgación entre la Entidad y entidades externas con las cuales se intercambie información e implementar controles de seguridad al monitoreo de la red.

- ✔ El proceso de TI implementa y mantiene la separación de las redes virtuales para garantizar la confidencialidad de la información en la red de telecomunicaciones de la Entidad.

- ✔ La transferencia de información deberá realizarse protegiendo la confidencialidad, integridad y disponibilidad de los datos de acuerdo con la clasificación del activo tipo información involucrada.

Políticas adquisición, desarrollo y mantenimiento de sistemas

- ✔ La Entidad busca que la Seguridad de la Información sea parte integral dentro ciclo de vida de desarrollo de los sistemas de información y en la adquisición de aquellos que presten servicios a la Entidad, para ello establece el procedimiento de desarrollo seguro de software, la revisión técnica y de seguridad de las aplicaciones para detectar vulnerabilidades antes de salir a producción y la aplicación del procedimiento gestión de cambios.

- ✔ La Entidad asegura que se diseñe e implemente los requerimientos de seguridad en el software, ya sea desarrollado o adquirido, que incluya controles de autenticación, autorización y auditoría de usuarios, verificación de los datos de entrada y salida, y que implemente buenas prácticas de desarrollo seguro.

- ✔ La Entidad establece controles técnicos para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información que son públicos mediante herramientas de seguridad perimetral de proveedores o de forma local.

- ✔ La Entidad cuenta con un ambiente de desarrollo y de pruebas seguro o, en su defecto, exige al proveedor mediante los contratos, que éste cuente con los controles de seguridad de la información sobre los ambientes.

- ✔ Los datos de pruebas que se utilicen durante todo el ciclo de vida de los sistemas de información deben ser seleccionados, utilizados y eliminados de forma segura.

Políticas relaciones con los proveedores

- ✔ Para proveedores críticos de tecnología, así como de procesos misionales, la Entidad exige que cuente con planes de continuidad de negocio y recuperación de desastres definidos e implementados, de modo que el proveedor contratado pueda responder ante eventuales escenarios que afecten el suministro de servicios o productos a la Entidad.

- ✔ La Entidad controla las relaciones con proveedores, y en particular aquellos que tienen acceso a la información. La información está suficientemente protegida con base a los acuerdos y contratos correspondientes. Esta protección debe contemplarse antes, durante y a la finalización del servicio.

- ✔ Cualquier cambio que se realice con algún proveedor crítico de TI o de los procesos misionales, debe aplicarse mediante el procedimiento de gestión de cambios establecido en la Entidad.

- ✔ La Entidad realiza revisiones periódicas al cumplimiento de las Políticas de Seguridad y Privacidad de la Información a los Proveedores.

Políticas gestión de incidentes

- ✔ La Entidad debe asegurarse que todos los servidores públicos y contratistas conozcan y aplican un procedimiento rápido y eficaz para actuar ante cualquier incidente en materia de seguridad de la información. Por lo tanto, se debe establecer los mecanismos para registrar los incidentes con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro.

- ✔ En la gestión del incidente y cuando sea necesario obtener evidencia de un incidente, siempre se debe garantizar el cumplimiento de los requisitos legales aplicables o comunicar a un ente competente para que realice el debido proceso.

- ✔ La Entidad establece y ejecuta procedimientos para identificar, analizar, valorar y dar un tratamiento adecuado a los incidentes, y que se hace una adecuada evaluación del impacto en el negocio de los incidentes de seguridad de la información.

- ✔ La Entidad debe establecer los mecanismos para registrar los incidentes con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro.

- ✔ La Entidad cuenta con una bitácora de los incidentes de seguridad de la información reportados y atendidos.

Políticas cumplimiento

- ✔ La Entidad gestiona la seguridad de la información de tal forma que se dé cumplimiento adecuado a la legislación vigente. Para esto, analiza los requisitos legales aplicables a la información, incluyendo los derechos de propiedad intelectual, protección de datos personales, los tiempos de retención de registros y los delitos informáticos.

- ✔ La Entidad asegura el conocimiento y cumplimiento de las obligaciones legales en materia de seguridad de la información. Por lo anterior, garantiza el cumplimiento de los derechos de propiedad intelectual de terceros controlando la adquisición y uso del software en la Entidad. Debe determinar las responsabilidades para gestionar la protección de datos personales.

Política de continuidad, contingencia y recuperación de la información

El objetivo de estas es garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información, para la alcaldía distrital

- ✔ El coordinador de sistemas o quien haga sus veces, es el responsable de la ejecución del plan de contingencia con el apoyo del equipo de trabajo de la Oficina de Sistemas.

- ✔ La copia de los datos almacenados en las estaciones de trabajo, son responsabilidad de cada uno de los usuarios.

- ✔ Se realizan copias del sitio Web Institucional como mínimo cada siete días, o según las actividades o publicaciones realizadas.

- ✔ Todo equipo que ingrese a la sesión de soporte y mantenimiento y/o deba ser intervenido, en forma que su información se pueda ver comprometida, se le debe realizar una copia de respaldo, sobre todo en aquellos archivos que el usuario manifieste su sensibilidad e importancia para la entidad.

PRIVACIDAD Y CONFIDENCIALIDAD

Política de tratamiento y protección de datos personales

Generalidades

De acuerdo con la definición establecida en la Ley 1581 de 2012, el dato personal es cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables, como el nombre, la edad, el sexo, el estado civil, el domicilio, entre otros.

Estos datos pueden almacenarse en cualquier soporte físico o electrónico y ser tratados de forma manual o automatizada.

La Ley 1266 de 2008 define los siguientes tipos de datos de carácter personal: Privado, Semiprivado y Público.

Adicionalmente la Ley 1581 de 2012 establece las siguientes categorías especiales de datos personales: Sensibles y personales de los niños, niñas y adolescentes.

También la ley define los siguientes roles:

a) **Responsable de 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 los datos".
b) **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". En cumplimiento de la de Ley 1581 de 2012 y reglamentada parcialmente por el Decreto Nacional 1377 de 2013, por la cual se dictan disposiciones para la protección de datos personales, la Alcaldía Distrital de Buenaventura además de ser la autoridad de protección de datos personales tiene la calidad de responsable del Tratamiento frente a las bases de datos creadas por la entidad. Adicionalmente, el Decreto reglamentario 1377 de 2013 define que los responsables deberán conservar prueba de la autorización otorgada por los Titulares de datos personales para el Tratamiento de los mismos.

Tratamiento y finalidades

El tratamiento que realizará la Alcaldía Distrital de Buenaventura será el de recolectar,

almacenar, procesar, usar y transmitir o transferir (según corresponda) los datos personales, atendiendo de forma estricta los deberes de seguridad y confidencialidad ordenados por la Ley 1581 de 2012 y el Decreto 1377 de 2013, con las siguientes finalidades:

a) Registrar la información de datos personales en las bases de datos de la Alcaldía Distrital, con la finalidad de analizar, evaluar y generar datos estadísticos, así como indicadores sectoriales para la formulación de políticas públicas.
b) Facilitar la implementación de programas en cumplimiento de mandatos legales.
c) Enviar la información a entidades gubernamentales o judiciales por solicitud expresa de las mismas.
d) Soportar procesos de auditoría externa e interna.

Así mismo, el Distrito suministrará los datos personales a terceros que le provean servicios o con quien tenga algún tipo de relación de cooperación, a fin de:

a) Brindar asistencia técnica.
b) Manejar y administrar Bases de Datos.
c) Dar respuestas a peticiones, quejas y recursos.
d) Dar respuestas a organismos de control.

Derechos del titular de los Datos Personales

a) Conocer, actualizar y rectificar sus datos personales frente a los responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.
b) Solicitar prueba de la autorización otorgada al responsable del Tratamiento salvo cuando expresamente se exceptúa como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la citada ley.
c) Ser informado por el responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales.
d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la Ley 1581 de 2012 y las demás normas que la modifiquen, adicionen o complementen.
e) Solicitar la supresión del dato cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales, el cual procederá

cuando la autoridad haya determinado que la Alcaldía Distrital de Buenaventura en el tratamiento ha incurrido en conductas contrarias a la Constitución y la normatividad vigente.

f) 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 el responsable o Encargado han incurrido en conductas contrarias a la ley y a la Constitución.
g) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

Disponibilidad del servicio e información

La Alcaldía Distrital de Buenaventura con el objetivo de facilitar a los usuarios el acceso a la información relativa a la gestión adelantada en los proyectos y actividades, actualiza de manera diaria el portal web.

La información entregada a los medios de comunicación debe hacerse a través del funcionario encargado del manejo de la comunicación, en este caso el director de la Oficina de Prensa y Comunicaciones.

Los datos que se publican en el portal web provienen de múltiples fuentes, los cuales están protegidos por la Ley. La entidad pone este material a disposición de los usuarios en forma individual, como licencia de usuario final, queda por lo tanto prohibida toda comercialización o usufructo de ese derecho de acceso.

La Alcaldía Distrital de Buenaventura autoriza el uso de la información contenida en el portal web, siempre y cuando se realice la cita textual. Queda en cambio prohibida la copia o reproducción de los datos en cualquier medio electrónico (Redes, Bases de Datos, CD Rom) que permita la disponibilidad de esta información a múltiples usuarios sin el visto bueno de la entidad por medio escrito.

Copias de seguridad

Las copias de seguridad, varía según la utilidad de la información de la entidad, donde: La información contenida en aplicativos como Finanzas e Impuestos se deben de realizar copias espejos, la información de aplicativo como Nómina se debe de realizar copia de seguridad diferencial diaria, la información contenida en aplicativo de Contratación se debe realizar copia de seguridad incremental diaria.

Las copias de seguridad serán almacenadas en servidores alternos, se realizarán copias totales de todos los aplicativos una vez por semana y se conservarán por un

mes y del último mes se conservarán por un año, es decir, en un mes se realizarán copias incrementales diariamente y 4 copias totales semanales. Cada copia total se conservará durante un mes y la última copia total de cada mes durante un año.

	ELABORÓ	REVISÓ	
FIRMA:			
NOMBRE:	**Ing. DEIVI ROBERTO LEÓN**	**Ing. JAIR H. CALIMEÑO**	
CARGO:	Prof. de Apoyo	Asesor TIC	

WEBGRAFÍA

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

MinTIC. Ley 1581 de 2012.

Recuperado de https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

MinTIC. Decreto 1078 de 2015.

Recuperado de https://www.mintic.gov.co/portal/604/articles-9528_documento.pdf

MinTIC. Modelo de Seguridad.
Recuperado de Marco de Referencia de Arquitectura Empresarial para la Gestión