POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Junio 2021

Tabla de contenido

INTRODUCCIÓN 4
1. OBJETIVO 5
2. ALCANCE 5
3. TÉRMINOS Y DEFINICIONES 5
4. MARCO LEGAL 8
5. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 10
6. POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. 10
6.1. POLÍTICAS DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. 10
Organización interna 10
Dispositivos móviles, teletrabajo, trabajo en casa. 11
6.2. POLÍTICA DE SEGURIDAD DE LOS RECURSOS HUMANOS 11
Antes de asumir el cargo. 11
Durante la ejecución del empleo. 12
Terminación y cambio de empleo. 12
6.3. POLÍTICA DE GESTIÓN DE ACTIVOS 12
Responsabilidad por los activos. 12
Clasificación de la Información. 13
Manejo de medios 13
6.4. POLÍTICA DE CONTROL DE ACCESO 14
Requisitos del negocio para control de acceso 14
Gestión de acceso a usuarios 14
Responsabilidades de los usuarios 15
Control de acceso a sistemas de información. 15
6.5. POLÍTICA PARA EL USO DE LOS RECURSOS CRIPTOGRAFICOS 15
Controles criptográficos 15
6.6. POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO 16
Áreas seguras 16
Equipos 16
6.7. POLÍTICA DE SEGURIDAD DE LAS OPERACIONES 17
Procedimientos operacionales y responsabilidades. 17
Protección contra código malicioso 17

Copias de respaldo 18
Registro y seguimiento 18
Control de software operacional 19
Gestión de Vulnerabilidades técnicas 19
Consideraciones sobre auditorias de sistemas de información. 19
6.8. POLÍTICA DE SEGURIDAD DE LAS COMUNICACIONES 19
Gestión de la seguridad de las redes 19
Transferencia de la Información. 20
6.9. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS 20
Requisitos de seguridad de los sistemas de información. 20
Seguridad en los procesos de desarrollo y de soporte 20
Datos de prueba 21
6.10. RELACIÓN CON LOS PROVEEDORES 21
Seguridad de la información en las relaciones con los proveedores. 21
Gestión de la prestación de los servicios de proveedores 22
6.11. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 22
6.12. POLÍTICA DE GESTIÓN CONTINUIDAD DEL NEGOCIO 22
Continuidad de la seguridad de la información 22
Redundancia 23
6.13. CUMPLIMIENTO 23
Cumplimiento de requisitos legales y contractuales 23
Revisiones de seguridad de la Información 23
CONTROL DE CAMBIOS 24

INTRODUCCIÓN:

La Alcaldía Distrital de Barranquilla, reconoce la importancia de la información, debido a que es uno de los activos más significativos para su funcionamiento y que tiene el deber y la responsabilidad de proteger y salvaguardar de una manera segura, garantizando su disponibilidad, integridad y confidencialidad, la cual es esencial para proporcionar servicios eficientes a los ciudadanos.

De igual manera, es consciente de las amenazas que enfrenta la información y de las consecuencias a las que se expone cuando no cuente con las medidas de seguridad y protección adecuadas. En ese sentido, la Alcaldía Distrital de Barranquilla tiene la responsabilidad de proteger la información y prevenir su mal uso tomando como marco de referencia lo establecido en las leyes **1273 de 2009**, **1581 de 2012, 1712 de 2014, el Decreto 1377 de 2013 y** la norma ISO 27001 para establecer políticas de seguridad que garanticen la confidencialidad de la información personal de los ciudadanos, empleados, directivos, proveedores y, en general, información relacionada con sus propias operaciones.

Teniendo en cuenta lo anterior, el presente instrumento tiene como finalidad establecer lineamientos para la aplicación de mecanismos que eviten la vulneración de la seguridad y privacidad de la información, una labor prioritaria que anima a todos a velar por el cumplimiento de las políticas definidas en este documento.

1. OBJETIVO

Establecer lineamientos necesarios, con el fin de fortalecer la seguridad y privacidad de la información de la Alcaldía Distrital de Barranquilla, enmarcados en la implementación de un Sistema de Gestión de la Seguridad de la Información, basados en la identificación de riesgos asociados a ella, propendiendo por la protección de su confidencialidad, integridad, disponibilidad, privacidad, continuidad, autenticidad.

2. ALCANCE

Los lineamientos contenidos en la presente política son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los servidores públicos, contratistas, visitantes y terceros que presten sus servicios o tengan alguna relación con la entidad a través de la recolección, procesamiento, almacenamiento, recuperación, intercambio de información, interno o externo en el cumplimiento de los objetivos institucionales de la Alcaldía Distrital de Barranquilla.

3. TÉRMINOS Y DEFINICIONES

Activos: cualquier cosa que tenga valor para la organización es considerada un activo, en este caso la información es un activo.

Administración de Riesgos: Se entiende por administración de riesgos, como el proceso de identificación, control, minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar la información o impactar de manera considerable la operación. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

Amenaza: causa potencial de un incidente no deseado, que puede producir un daño a un sistema.

Archivo o fichero informático: es un conjunto de bits que son almacenados en un dispositivo. Un archivo es identificado por un nombre y la descripción de la carpeta o directorio que lo contiene. A los archivos informáticos se les llama así porque son los equivalentes digitales de los archivos escritos en expedientes, tarjetas, libretas, papel o microfichas del entorno de oficina tradicional.

CAU: Centro de Atención a Usuarios.

Código malicioso: Es un código informático que crea brechas de seguridad para

dañar un sistema informático.

Confidencialidad: es la cualidad de la información por medio de la cual se garantiza que está disponible únicamente al personal autorizado para acceder a dicha información.

Control: Son todas aquellas políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Datacenter: Se denomina también Centro de Procesamiento de Datos (CPD) a aquella ubicación o espacio donde se concentran los recursos necesarios (TI) para el procesamiento de la información de una organización.

Disponibilidad: es la propiedad de estar accesible y utilizable al ser solicitado por una entidad autorizada.

Hardware: conjunto de componentes que integran la parte material de una computadora.

Home Office: Oficina en casa o trabajo en casa

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Incidente de seguridad: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información

Integridad: es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. Es la acción de mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

Malware: código maligno, software malicioso, software dañino o software malintencionado. Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

Política: su objetivo es establecer, a partir de la observación de hechos de la realidad política, principios generales acerca de su funcionamiento.

Privacidad de la información: El derecho que tienen todos los titulares de la

información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de Gobierno Digital la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Riesgo: es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

Sistema de Gestión de la Seguridad de la Información (SGSI): corresponde al diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Seguridad informática o de tecnologías de la información: es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta; especialmente la información contenida o circulante. Para ello existe una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos. archivos), hardware y todo lo que la organización valore (activo) y signifique un riesgo en el supuesto de que esta información confidencial llegue a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

Terceros: persona o entidad que se reconoce como independiente.

Usuarios: el usuario es aquella persona que usa una cosa o servicio habitualmente. En sentido general, un usuario es un conjunto de permisos y de recursos a los cuales se tiene acceso.

Vulnerabilidad: debilidad de un sistema que puede ser explotada por una o más amenazas

4. MARCO LEGAL

Constitución Política de Colombia. Artículo 15.

Ley 44 de 1993: Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).

Ley 527 de 1999: Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 594 de 2000: Por medio de la cual se expide la Ley General de Archivos.

Ley 850 de 2003: Por medio de la cual se reglamentan las veedurías ciudadanas

Ley 1266 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 la proveniente de terceros países y se dictan otras disposiciones.

Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, 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, entre 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, se crea la agencia Nacional de espectro y se dictan otras disposiciones.

Ley 1437 de 2011: Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.

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 la cual se dictan disposiciones generales para la protección de datos personales.

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 1915 de 2018: Por la cual se modifica la Ley 23 de 1982 y se establecen

otras disposiciones en materia de derecho de autor y derechos conexos.

Ley 1952 de 2019: Por medio de la cual se expide el código general disciplinario

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 0884 del 2012: Por el cual se reglamenta parcialmente la Ley 1221 del 2008. **Decreto 1377 de 2013:** Por el cual se reglamenta parcialmente la Ley 1581 de 2012. **Decreto 886 de 2014:** Por el cual se reglamenta el Registro Nacional de Bases de Datos.

Decreto 103 de 2015: Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

Decreto 1074 de 2015: Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.

Decreto 1078 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.

CONPES 3854 de 2016. Política Nacional de Seguridad digital.

Ley 1978 de 2019: Por la cual se moderniza el Sector de las Tecnologías de la Información y las Comunicaciones -TIC, se distribuyen competencias, se crea un Regulador Único y se dictan otras disposiciones

5. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Alcaldía Distrital de Barranquilla, conociendo de la importancia de una adecuada gestión de la información, se ha comprometido a proteger, preservar y administrar la confidencialidad, integridad, disponibilidad de la información de la Entidad, mediante una gestión integral de riesgos, implementación de controles, previniendo incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua.

Para asegurar la dirección estrategia de la Alcaldía Distrital de Barranquilla se establecen los siguientes objetivos:

- Minimizar el riesgo de vulnerabilidad en la seguridad de la información en los procesos de la entidad.
- Cumplir con los principios de Disponibilidad, integridad y confidencialidad de la seguridad de la información.
- Mantener la confianza de los servidores, contratistas y terceros
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Verificar de manera periódica el cumplimiento de la política de seguridad y privacidad de la información.
- Propender para que los servidores, contratistas y terceros cumplan con las políticas, directrices y buenas prácticas definidas en este documento.

6. POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

6.1. POLÍTICAS DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

Organización interna

- La entidad conformará un *'Grupo interno de trabajo de Seguridad y Privacidad de la Información'*, con roles definidos y la responsabilidad de identificar, validar y definir lineamientos en temas de seguridad.
- Los deberes de cada dependencia, se definirán en los actos administrativos publicados en la gaceta distrital.
- La Gerencia TIC mantendrán contacto con los organismos, grupos de

interés y autoridades competentes, con el fin de solicitar el apoyo en caso de presentarse un incidente de seguridad de la información.
- Los proyectos que se desarrollen en la estructura central de la administración del distrito de Barranquilla, contemplarán una gestión de riesgos de seguridad asociados a la información del proyecto. (Identificación del riesgo y la forma como serán gestionados).

Dispositivos móviles, teletrabajo, trabajo en casa.

- La Gerencia TIC, mantendrá actualizado el inventario de los equipos asignados y las especificaciones requeridas, para realizar trabajo en casa, o funciones que requieran salida de los equipos de la entidad.
- Todos los equipos que almacenan información de la Alcaldía, deben tener instalado antivirus y demás aplicativos requeridos actualizados.
- En caso de pérdida o robo del equipo o dispositivo móvil asignado para el cumplimiento de las funciones tendrá que realizar la respectiva denuncia ante la entidad competente e informar al jefe inmediato para el trámite pertinente.
- Los recursos tecnológicos asignados a los usuarios, como el acceso a Internet y el correo electrónico son exclusivos para ejercer funciones de trabajo.
- La Gerencia de la TIC, definirá los requerimientos para autorizar conexiones remotas o locales a la infraestructura tecnológica necesarias para el cumplimiento de las funciones de servidores, contratistas y terceros.
- Toda la información gestionada y accedida remotamente será utilizada solo para el cumplimiento de las funciones o de las obligaciones contractuales.

6.2. *POLÍTICA DE SEGURIDAD DE LOS RECURSOS HUMANOS*.

Antes de asumir el cargo.

- Las secretarias Distrital de Gestión Humana y General definirán los procedimientos en los cuales se verifiquen los antecedentes requeridos para el ejercicio de los cargos públicos y las obligaciones contractuales de los contratistas de la administración de acuerdo con la normatividad vigente.
- Las áreas encargadas de la vinculación de servidores, contratistas y terceros establecerán los controles necesarios para proteger la confidencialidad y reserva de la información contenida en las historias laborales y expedientes contractuales.
- En los términos y condiciones de vinculación se incluirán los acuerdos de

confidencialidad y no divulgación de la información reservada.

Durante la ejecución del empleo.

- En los procesos de inducción y reinducción se incluirá los temas relacionados con seguridad de la información y protección de datos personales.
- La Secretaría Distrital de Comunicaciones en apoyo con las áreas pertinentes incluirán en el plan de comunicaciones campañas en pro de la toma de concientización de la seguridad de la información.
- La Oficina de Control Interno Disciplinario incluirá en sus procedimientos actividades relacionadas con el incumplimiento de la presente política.

Terminación y cambio de empleo.

- Las secretarias Distrital de Gestión Humana y General definirán en los procedimientos de terminación de contratos, las responsabilidades y deberes en la seguridad de la información.
- Es responsabilidad del servidor, contratista o tercero entregar la información gestionada durante del ejercicio de sus funciones, cuando se presente novedad de retiro, investigación, inhabilidades o cambio de funciones.
- El interventor del contrato o quien haga sus veces será el responsable de custodiar la información del contratista en caso de terminación anticipada, definitiva, temporal o cesión del contrato.
- La Gerencia TIC será el responsable de mantener actualizado el inventario de activos de tecnología e información, así como el control de acceso a sistemas de información y servicios.

6.3. POLÍTICA DE GESTIÓN DE ACTIVOS

Responsabilidad por los activos.

- Todos los procesos deben contar con un inventario de activos de tecnología e información, y evidenciar a través de los instrumentos dispuestos.
- La Gerencia de las TIC y la Oficina de Gestión Documental definirán los lineamientos requeridos para el manejo de los activos de tecnología e información relacionados en los instrumentos dispuestos.
- Los servidores públicos, contratistas y terceros deben hacer entrega de los activos bajo su responsabilidad en el formato definido para ello, al finalizar el empleo o contrato.

Clasificación de la Información.

- La Gerencia TIC, y el área de Gestión documental clasificarán los activos de información conforme a lo establecido en los instrumentos de la entidad.
- Las Tablas de Retención Documental (TRD) deben indicar el tipo de clasificación de las series, subseries y documentos en ella contenidas.
- Cada propietario del activo de Información debe velar por el cumplimiento de su clasificación de acuerdo con lo establecido en los procedimientos diseñados para el manejo de activos de tecnologías e Información

Manejo de medios

- La Gerencia de las TIC, debe generar instructivo o procedimiento para la gestión y uso de medios removibles.
- Todo medio removible debe ser escaneado por el antivirus, antes de introducirlo en los equipos de cómputo de la Alcaldía Distrital de Barranquilla.
- Es responsabilidad de servidores, contratistas y terceros tomar las medidas para la protección de la información contenida en medios removibles, con el fin de evitar el acceso no autorizado, daños y perdida de información.
- Se prohíbe el uso de medios removibles que contengan información clasificada y reservada de la Alcaldía.
- La Gerencia de las TIC debe generar y aplicar lineamientos para la disposición segura de los dispositivos que almacenen información de la entidad, ya sea cuando son dados de baja o asignados a un nuevo usuario.
- Se deben emplear herramientas de borrado seguro y demás mecanismos de seguridad pertinentes en los medios de propiedad de la Alcaldía que sean reutilizados o dados de baja, con el fin de controlar que la información contenida en estos medios no se pueda recuperar
- La oficina de logística en conjunto con la Gerencia TIC, mantendrá actualizado el procedimiento de disposición final de los RAEE, según la normatividad vigente.

6.4. POLÍTICA DE CONTROL DE ACCESO

Requisitos del negocio para control de acceso

- La Gerencia de las TIC administrará y controlará los accesos a todos los servicios de TI, de acuerdo al procedimiento establecido
- La conexión remota a la red de la Alcaldía debe hacerse a través de VPN, la cual debe ser aprobada, registrada y monitoreada por la Gerencia TIC.
- La Gerencia de las TIC para los eventos que se realicen en la entidad debe generar usuario y clave Wifi, el cual debe expirar una vez finalizado el evento.
- El usuario de los sistemas de información y los servicios debe ser igual al usuario del dominio y cumplir con los requisitos establecidos en el procedimiento creación de usuario.
- La Gerencia de las TIC debe revisar que los equipos personales de servidores, contratistas o terceros que se conecten a la red de la Alcaldía, cumplan con los requisitos para autenticarse y podrán realizar las tareas para los cuales fueron autorizados.

Gestión de acceso a usuarios

- La Gerencia de la TIC y líderes de proceso, administrarán (crear, actualizar e inactivar) las cuentas de usuarios, privilegios y autenticación de estas, en los sistemas de información y servicios de TI que lo requieran de acuerdo al procedimiento establecido
- La Gerencia de las TIC, solo otorgará a los usuarios, los accesos solicitados y autorizados por el nivel directivo de la administración.
- La Gerencia de las TIC llevará el control de todas las cuentas de usuarios con el fin unificar y estandarizar el acceso de los usuarios a las diferentes plataformas y sistemas de información de la Alcaldía Distrital de Barranquilla.
- Sólo se otorgan los privilegios para la administración de recursos tecnológicos, servicios de red, sistemas operativos y sistemas de información a aquellos usuarios que realicen actividades de administración de servicios de TI.
- Es obligación del nivel directivo del área verificar permanentemente el nivel de acceso de sus funcionarios, contratistas y terceros a los sistemas información de la entidad y servicios de TI. Cualquier cambio en los niveles de acceso existentes debe solicitarse a la Gerencia TIC
- La Gerencia TIC y los líderes de proceso serán los responsables de mantener actualizado los derechos de acceso de funcionarios, contratistas y terceros a los sistemas de información y servicios TIC, al finalizar su empleo, contrato o cuando se hagan cambios de funciones

asignadas.

- El usuario y la contraseña asignados para el acceso a los diferentes servicios tecnológicos, es personal e intransferible. Cualquier actividad que se realice con el usuario y clave será responsabilidad del servidor público y contratista al cual le fue asignado.
- Es responsabilidad de los usuarios salvaguardar sus credenciales de acceso a sistemas operativos, aplicaciones, bases de datos y correo. Los usuarios no deben compartir estas credenciales.
- Todas las claves deben estar pre expiradas al momento de su creación, forzando al usuario a cambiarla una vez ingrese al sistema cuando se use por primera vez o al resetearla.

Responsabilidades de los usuarios

- La Gerencia de las TIC debe garantizar que los usuarios, realicen el cambio de contraseña de acceso a los servicios cada vez que sea requerido.

Control de acceso a sistemas de información.

- Solo tendrán acceso a los sistemas de información aquellos usuarios que por sus funciones así lo requieran, con el visto bueno de su jefe inmediato, del usuario líder responsable del sistema de información correspondiente y el Gerente de las TIC.
- La Gerencia de las TIC debe deshabilitar los servicios o funcionalidades no utilizadas de los sistemas operativos, bases de datos y demás recursos tecnológicos. Así mismo restringir el uso de programas utilitarios que puedan afectar la seguridad de la información.
- La Gerencia de las TIC, establecerá los controles necesarios para restringir el acceso a código fuente de las aplicaciones realizadas en la Alcaldía.

6.5. POLÍTICA PARA EL USO DE LOS RECURSOS CRIPTOGRAFICOS

Controles criptográficos

- La Gerencia de las TIC, debe implementar controles criptográficos para proteger de claves de acceso a sistemas de información, datos y servicios dando cumplimiento a la normatividad vigente.

- La Gerencia de las TIC, debe verificar que todo sistema de información

que requiera almacenar y/o transmitir información clasificada o reservada cuente con mecanismos de cifrado de datos.

- El administrador de cada sistema de información será responsable de la activación, recepción, distribución y protección de las llaves criptográficas a los usuarios autorizados y velará porque la llave se encuentre activa en el periodo de tiempo previsto.

6.6. POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

Áreas seguras

- La Gerencia de la TIC y los líderes de proceso de áreas restringidas, definirá los mecanismos para el control de acceso y protección de las áreas que manejen infraestructura e información crítica o sensible.
- La Secretaría General con el apoyo del personal de vigilancia debe registrar en una bitácora o sistema de información el ingreso y retiro de todo equipo cómputo elemento informático (pc o portátil, mouse, teclado, cargador, etc.), servidores y equipos activos de red; en caso de que estos equipos sean propiedad de la Alcaldía deberán contar con autorización expresa de las áreas correspondientes y en el formato de orden de salida.
- La Secretaría de Gestión humana y dependencias relacionadas diseñarán e implementarán el plan de preparación para prevención y respuesta ante emergencias con el fin de mitigar el impacto ante un evento catastrófico.
- La Secretaría General garantizará que todos los puntos de ingreso o acceso a las instalaciones estarán vigilados para controlar el ingreso de personal no autorizada.

Equipos

- Los servidores, contratistas o terceros velarán por que los computadores y dispositivos a su disposición estén protegidos contra la intemperie, en especial los que se encuentren ubicados en sitios expuestos a polvo y humedad o que, por razones de brigadas o actividades propias de cada dependencia, tengan que trasladarse a sitios distintos a donde fueron instalados para su habitual funcionamiento.
- La Gerencia de las TIC establece los mecanismos para la protección y el uso del cableado estructurado y la red de energía regulada en los puestos de trabajo y centros de datos en los cuales solo deben conectar equipos de cómputo y telecomunicaciones, los otros elementos deben conectarse a la red eléctrica no regulada.
- La Gerencia de TIC, establecerá plan de mantenimiento preventivo de los activos de tecnología e información para asegurar su disponibilidad e

integridad.

- Cuando un equipo o medio extraíble sea reasignado o retirado de servicio, la Gerencia de las TIC debe garantizar la eliminación de toda información mediante mecanismos de borrado seguro teniendo en cuenta que previo a esta actividad debe realizarse una copia de seguridad de esta.
- Los Servidores Públicos, contratista o terceros de la Alcaldía, deben bloquear la pantalla del computador a su cargo cuando se ausenten de su puesto de trabajo, para impedir el acceso de terceros no autorizados a la información almacenada en el equipo de cómputo.
- Los Servidores Públicos, contratista o terceros de la Alcaldía, deben mantener los escritorios limpios, en orden, libres de documentos y medios de almacenamiento removibles, para impedir el acceso no autorizado a la información.

6.7. POLÍTICA DE SEGURIDAD DE LAS OPERACIONES

Procedimientos operacionales y responsabilidades.

- La Gerencia de las TIC y demás dependencias documentarán y actualizarán los procedimientos operativos para garantizar la disponibilidad, integridad y confidencialidad de la información y registrarán los cambios en el aplicativo ISOLUCION, para conocimiento de servidores, contratistas y terceros de la entidad.
- La Gerencia de las TIC definirá procedimiento para el monitoreo de la capacidad tecnológica y elaborará proyecciones futuras para optimizar el desempeño de la operación de la entidad.
- La Gerencia de las TIC garantizará la infraestructura necesaria para separar los ambientes de desarrollo, prueba y operación de los aplicativos y servicios. Los ambientes de desarrollo y prueba mantendrán los controles de seguridad establecidos en el ambiente de operación.

Protección contra código malicioso.

- La Gerencia de las TIC establecerá los controles para la detección, prevención y recuperación contra códigos maliciosos. Además, proporcionará los mecanismos para generar cultura de seguridad entre los Servidores Públicos, contratistas y terceros frente a los ataques de software malicioso.
- La Gerencia de las TIC contará con herramientas tales como antivirus, antimalware, antispam y antispyware que reduzcan el riesgo de contagio de software malicioso. Además, que dichas herramientas cuenten con las licencias de uso requeridas.

- La Gerencia de las TIC velará por que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus.
- La Gerencia de las TIC velará que el software de antivirus, antispyware, antispam y antimalware posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.
- Los servidores públicos, contratista o terceros, se abstendrán de abrir o ejecutar archivos y/o documentos de fuentes desconocidas especialmente los que se encuentran en medios de almacenamiento externo o que provienen de correos electrónicos desconocidos.
- Los servidores públicos, contratista o terceros que sospechen o detecten alguna infección por software malicioso deben notificar de inmediato a la gerencia de las TIC a través de los canales establecidos, con el fin de ejercer los controles correspondientes
- Los servidores públicos, contratista o terceros que ingresen a la red de comunicaciones de la Alcaldía de Barranquilla, deberán ejecutar el antivirus aprobado y actualizado por la Entidad. Si el computador no tiene instalado antivirus, debe informar a la Gerencia TIC quien indicará el antivirus a utilizar según listado de software permitidos.

Copias de respaldo

- La Gerencia de las TIC definirá y documentará un procedimiento de copias de respaldo y restauración de la información, donde se establezca el esquema, de qué, cómo, quién, con qué periodicidad, tipo de respaldo y nivel de criticidad. Dicho procedimiento debe cobijar los equipos dentro y fuera de la entidad y la información almacenada en equipos personales.
- La información de los servidores y demás sistemas serán respaldados mediante un método de copia de seguridad adecuado, igualmente, se debe utilizar un medio de almacenamiento apropiado.
- La Gerencia de las TIC, velará por que los medios magnéticos que contienen la información sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con la seguridad física y medioambiental apropiada.
- Las copias de seguridad que se realicen periódicamente serán sometidas a prueba, para verificar o validar el restablecimiento de los datos.

Registro y seguimiento

- Los sistemas de información y aplicaciones de la Gerencia de las TIC deben elaborar registros '*log'* o de eventos de administradores, operadores y usuarios, los cuales se deben conservar, proteger y revisar regularmente, al igual que los registros de eventos generados por otros

sistemas de información y servicios de tecnología.

- La Gerencia TIC debe garantizar que los relojes de toda la infraestructura tecnológica de la entidad estén sincronizados con una única fuente de tiempo.

Control de software operacional

- La Gerencia de las TIC designará responsables y establecerá instructivos y guías para controlar la instalación de software en sistemas operativos
- Los servidores, contratistas y terceros no están autorizados para descargar e instalar programas o software. En caso de ser requeridos para realizar funciones propias de la Alcaldía, debe informar a la Gerencia TIC quien hará las gestiones necesarias para la instalación teniendo en cuenta el listado de software permitido.

Gestión de Vulnerabilidades técnicas

- La Gerencia de las TIC, debe establecer en el procedimiento de gestión de riesgos las herramientas para identificar y evaluar las vulnerabilidades técnicas de los sistemas de información y elaborar el plan de tratamiento de los riesgos asociados a las vulnerabilidades.

Consideraciones sobre auditorias de sistemas de información.

- Las auditorías a los sistemas operativos deben ser planificadas y socializadas a las partes interesadas, con el fin de minimizar las interrupciones en la ejecución de las actividades diarias.

6.8. POLÍTICA DE SEGURIDAD DE LAS COMUNICACIONES

Gestión de la seguridad de las redes

- La Gerencia de las TIC debe revisar periódicamente todos los elementos que conforman la red de comunicaciones, los mecanismos de seguridad y los acuerdos de nivel de servicios para garantizar la operación de la entidad; en caso de detectar una falla o anomalía se toman los correctivos del caso y se deben registrar en una bitácora para llevar trazabilidad de estos.

Transferencia de la Información.

- La Gerencia de las TIC y la oficina de Gestión Documental definirán, implementarán y revisaran periódicamente la política de protección de datos personales, donde se establecen las directrices para la trasmisión y transferencia de información, mediante el uso de cualquier medio de comunicaciones.
- Es responsabilidad de los usuarios que manejan información confidencial y sensible de la Alcaldía de Barranquilla, dar el tratamiento que propendan por su protección, y hacer uso de herramientas criptográficas y certificados electrónicos en transacciones vía Web o correos electrónicos previamente proporcionados por la Entidad.
- La herramienta de correo electrónico utilizará un filtro corporativo para evitar que se reciba contenido malicioso.
- Todos los mensajes de correo electrónico emitidos por usuarios de Alcaldía de Barranquilla o sus Entidades Adscritas que sean dirigidos a direcciones de correo externas, que contengan información confidencial, deben incluir una nota que haga referencia a la seguridad de la información y protección de datos personales.

6.9. *ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS*.

Requisitos de seguridad de los sistemas de información.

- La Gerencia de las TIC establecerá e implementará metodologías para el desarrollo y mantenimiento de software seguro, que incluyan la definición de requisitos de seguridad y privacidad de la información, en software nuevo o existentes.
- En el proceso de análisis y adquisición de software a terceros o contratista, se debe considerar aspectos y atributos de seguridad de la información, y el impacto en la seguridad frente a eventuales cambios o modificaciones para su implantación en la Alcaldía de Barranquilla.
- La información compartida en la red estará protegida con mecanismos de seguridad perimetral, conexiones VPN, aplicaciones en dominios propios y protocolos seguros, y en las redes públicas, en lo posible la información estará cifrada, aumentando la seguridad en las transacciones.

Seguridad en los procesos de desarrollo y de soporte

- La Gerencia de las TIC en el proceso de desarrollo y/o mantenimiento de software, debe contar con metodologías y lineamientos de desarrollo seguro para cada etapa del ciclo de vida: análisis, construcción, pruebas y puesta en producción. Durante cada etapa ejecutar y documentar

pruebas de funcionalidad de la seguridad y privacidad

- La Gerencia de las TIC, debe definir un procedimiento para el control de cambio que incluya revisión técnica y restricciones de las aplicaciones después de los cambios.
- La Gerencia de las TIC garantizará la seguridad para los ambientes de desarrollo seguro teniendo en cuenta los controles definidos en la política de seguridad de las operaciones.
- La Gerencia de las TIC, realizará supervisiones a los desarrollos y/o mantenimientos de software tercerizados velando que cumplan con la política y con las directrices establecidas.
- Los datos de prueba extraídos desde las bases de datos de los sistemas en producción sólo deben ser empleadas dentro de las instalaciones de la Alcaldía de Barranquilla y deben ser autorizadas por el dueño de la información, o en su defecto por la Gerencia de Control Interno y se deberá elaborar y formalizar un Convenio de Confidencialidad por parte de terceros.
- El acceso a las bases de datos de construcción, prueba y producción, deben contar con controles de acceso (autenticación y autorización). Debe definirse los roles de acceso a las bases de datos en sus diferentes ambientes y qué tipo de acceso (consulta, actualización, eliminación).

Datos de prueba

- El acceso a la documentación de sistemas de información, bibliotecas de códigos fuentes, datos de prueba y programas ejecutables, debe estar restringida sólo a personal autorizado. La excepción a esta política, son los manuales de usuario, manuales de capacitación, u otros documentos destinados a los usuarios de los sistemas de información.
- En los datos de prueba se debe mantener los mismos controles de seguridad de los datos operativos. Si existen información sensibles contenidos en los datos de pruebas, deberán ser modificado para evitar el reconocimiento del mismo. Finalizada las pruebas se debe elimina dicha información antes de su ejecución y puesta en marcha del sistema de información.

6.10. RELACIÓN CON LOS PROVEEDORES

Seguridad de la información en las relaciones con los proveedores.

- La Gerencia de las TIC y el área de Contratación definirán los requisitos

para el cumplimiento de las obligaciones contractuales relacionado con la Seguridad y Privacidad de la Información, riesgos asociados, los compromisos establecidos de confidencialidad y el cumplimiento de las políticas de seguridad de la información de la Alcaldía.

Gestión de la prestación de los servicios de proveedores

- La Gerencia de las TIC, realizará seguimientos periódicos al cumplimiento de los requisitos definidos en las obligaciones contractuales. Además, se debe mantener actualizado los acuerdos de servicios.

6.11. *GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN*.

- La gerencia de las TIC conformará comité técnico con roles y responsabilidades definidas para la gestión de la seguridad de la información en los sistemas de información, la infraestructura y servicios tecnológicos de la entidad.
- La Gerencia de las TIC establecerá un procedimiento para detectar, reportar, evaluar y responder a los incidentes de seguridad de la información de forma estructurada y planificada.
- Es responsabilidad de funcionarios, contratistas y terceros reportar cualquier vulnerabilidad de seguridad de la información observada o sospechada en los sistemas de información, infraestructura o servicios tecnológicos a través de los canales definidos por la Gerencia TIC.
- La gerencia de las TIC debe identificar y registrar las lecciones aprendidas y conocimiento adquirido al gestionar los incidentes de seguridad en las herramientas definidas por el área pertinente, con el fin de reducir la posibilidad o impacto de incidentes futuros. De igual forma identificará, recogerá y preservará la información que pueda servir como evidencia de incidentes, en caso de ser requerida por entes internos o externos.

6.12. *POLÍTICA DE GESTIÓN CONTINUIDAD DEL NEGOCIO*.

Continuidad de la seguridad de la información

- La gerencia de las TIC establecerá un procedimiento de continuidad de la seguridad de la información para planificar, implementar, verificar, revisar y evaluar la continuidad del negocio de la entidad en situaciones adversas.

Redundancia

- La Gerencia de las TIC, identificará el nivel de criticidad de los activos de tecnología para mantener la disponibilidad en la operación de los servicios.

6.13. CUMPLIMIENTO

Cumplimiento de requisitos legales y contractuales

- La Alcaldía Distrital de Barranquilla, gestiona la seguridad y privacidad de la información dando cumplimiento adecuado a la legislación vigente. Analizando los requisitos legales aplicables a la información de derechos de autor y propiedad intelectual, protección de datos personales, ley de transparencia y del derecho de acceso a la información pública. Igualmente, velará por la protección de los registros ante cualquier perdido, destrucción, falsificación acceso o liberación no autorizada de acuerdo con los requisitos legislativos, y contractuales de la Alcaldía.

Revisiones de seguridad de la Información

- La alcaldía Distrital de Barranquilla se asegurará de las revisiones independientes de la presente política, la misma debe ser planificada o gestionada cuando se presenten cambios significativos.
- Es responsabilidad de los líderes de procesos hacer revisiones periódicas y asegurar el cumplimiento de los procedimientos definidos, los cuales están relacionados con los controles establecidos en la presente política.
- La Gerencia las TIC, realizará revisiones técnicas planificadas a los activos de tecnología para determinar el cumplimiento de la presente política.
- El incumplimiento a las responsabilidades definidas en la presente política podrá generar la apertura de un proceso disciplinario de conformidad con la ley, sin perjuicio de la responsabilidad penal que puedan acarrear dichas conductas.
- La revisión de la presente política estará a cargo de la Gerencia de las TIC y será revisada cuando se considere necesario; sin embargo, el periodo no debe ser superior a un año.

CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
Noviembre 2016	2016	Se establece una nueva versión de la Política de Seguridad de la Información
Enero 2019	2019	*Se realizaron cambios en los numerales:* • Se amplía el ámbito de aplicación, adquisición, desarrollo, mantenimiento y seguridad de los sistemas de información, roles y responsabilidades, tratamiento y gestión de riesgos • *Cambia nombre de área de Gerencia de Sistemas a Oficina de Sistemas*
Junio 2021	2021	Se ajustan los numerales a la norma técnica ISO 27001

JAIME CRÍALES HENAO
Gerente Gerencia de las TICs – Despacho del Alcalde