OFICINA INFORMÁTICA Y TELEMÁTICA

POLITICA DE SEGURIDAD DE LA INFORMACIÓN (MSPI)

SANTIAGO DE CALI, AGOSTO DEL 2021

CONTENIDO

INTRODUCCION

Este documento contiene las Políticas de Seguridad de la Información definidas en el marco del desarrollo del proyecto "*Modelo de Seguridad y Privacidad de la Información*" (en adelante MSPI) para el Concejo Distrital de la Ciudad de Cali, estableciéndose así, como el núcleo principal del Modelo de Seguridad y privacidad.

Las políticas mencionadas en este documento son la base para la definición de instructivos, manuales, procedimientos y cualquier otra instrucción que propenda por la seguridad de los activos de información del Concejo Distrital de Cali, posibilitando la construcción de una arquitectura de seguridad sustentada en procesos homogéneos y estándares alineados con el marco normativo del Sistema de Gestión de Calidad del Concejo, que permitan la integración con la arquitectura de tecnología informática y con el modelo de administración y control de riesgos, que garanticen la seguridad de la información en el Concejo.

El cumplimiento de las Políticas de Seguridad de la Información es de carácter obligatorio y ningún servidor público, contratista, particular y/o tercero, está exento del cumplimiento de las políticas que aquí se encuentren definidas ya que estas cuentan con la aprobación en pleno del Comité de Gestión y Desempeño en cabeza del presidente del Concejo Distrital de Cali. Si un individuo o entidad viola las disposiciones en las Políticas de Seguridad de la Información, por negligencia o intencionalmente, el Concejo Distrital de Cali se reserva el derecho de tomar las medidas correspondientes, tales como acciones disciplinarias, despido, acciones legales, reclamo de compensación por daños, u otras que así contemple la ley[1].

[1] Ley 1273 de 2009: Ley de Delitos Informáticos, Ley 1581 de 2012: Protección de Datos Personales

OBJETIVOS

Objetivo General

El Concejo Distrital de la Ciudad de Cali, fundamenta el gobierno del Modelo de Seguridad y Privacidad de la Información en el establecimiento de lineamientos que permitan proteger, asegurar y salvaguardar la integridad, confidencialidad, disponibilidad y privacidad de los activos de información del Concejo de Cali, teniendo en cuenta aspectos organizacionales como procesos, la operación, objetivos, misión, visión y requerimientos legales y buenas prácticas que demanda el estado. Con su divulgación se busca que todos los servidores públicos, contratistas, particulares y/o terceros, conozcan de forma individual y colectiva la política de seguridad de la información y contribuyan al aseguramiento y trato adecuado de los activos de información del Concejo Distrital de Cali.

Objetivos Específicos

- Definir la política de seguridad privacidad de la información del Honorable Concejo Distrital de la Ciudad de Cali.
- Definir los lineamientos a ser tenidos en cuenta en el diseño e implementación del Modelo de Seguridad y Privacidad de la Información.
- Estar conforme y dar cumplimiento a directrices regulatorias y buenas practicas definidas por el estado colombiano, aplicables a la misión y función pública adelantada por el Concejo Distrital de la Ciudad de Cali.
- Salvaguardar los activos de información del Concejo Distrital de la Ciudad de Cali.
- Mantener actualizado el MSPI respecto a políticas, manuales, procedimientos, guías y estándares, a efecto de mantener su vigencia, idoneidad y eficacia en el aseguramiento de los activos de información del Concejo Distrital de Cali.
- Fomentar una cultura de seguridad de la información en todas las partes que intervienen dentro de los procesos misionales y de apoyo del Concejo Distrital de Cali como también terceros, proveedores y ciudadanos del común.
- Mantener la operabilidad y continuidad del negocio frente a la materialización de incidentes de seguridad, mediante la definición de una estrategia de continuidad de los procesos del Concejo Distrital de la Ciudad de Cali.

ALCANCE

La política de seguridad es una regla de definición general transversal a todo el Concejo, que abarca las directrices de seguridad lógica (tecnología), física (seguridad perimetral y recursos físicos) y conductual de los usuarios en el uso de los activos de información, que representa los objetivos sobre los que se sustenta el Modelo de Seguridad y Privacidad de la Información del Concejo Distrital de Cali. Debe estar alineada en pro de los objetivos y directrices por los que propende el concejo, está sujeta a revisiones y modificaciones ante cambios estructurales.

En la definición de las políticas se cubren aspectos regulatorios, administrativos y de control que deben acatar tanto los responsables en la administración del Modelo de Seguridad y Privacidad de la Información como todos los empleados que hacen parte de la labor del Concejo, terceros, proveedores y ciudadanos del común que utilizan los servicios provistos por Concejo, con el fin de lograr un adecuado nivel de confidencialidad, integridad, disponibilidad y privacidad de la información.

Estas políticas deben ser revisadas y en caso de necesitarse, ser actualizadas para garantizar que siguen siendo adecuadas, suficientes y eficaces en el aseguramiento de los recursos de información del Concejo Distrital de Cali.

MARCO REGULATORIO Y NORMATIVO

El Concejo Distrital de la Ciudad de Cali, como entidad de índole publica, se encuentra sujeto a un marco normativo y regulatorio en lo relacionado con la seguridad de la información, como también a las buenas practicas del mercado en materia de seguridad de la información definidas por entidades reconocidas en la emisión y normalización de metodologías y buenas prácticas a nivel mundial.

Se tiene como principal hoja de ruta las definiciones impartidas por el estado en su estrategia de Gobierno Digital, compulsada en el decreto 1008 de 2018 que modifica el decreto 1078 de 2015 "*Decreto Único Reglamentario del sector de tecnologías de la Información y las Comunicaciones*", dentro del cual destaca el propósito de garantizar la seguridad y la privacidad de la información como una de las iniciativas de la Subdirección de Estándares y Arquitectura de TI en la gestión e implementación adecuada del ciclo de vida de la seguridad de la información.

A continuación, se relacionan las normas, decretos y disposiciones legales que aplicables al Concejo Distrital de la Ciudad de Cali en lo concerniente al establecimiento del Modelo de Seguridad y Privacidad de la Información (MSPI):

- Ley 1266 de 2008 *"Por la cual se dictan las 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 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"*
- Decreto 2693 de 2012 *"Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia"*
- Ley 1581 de 2012 ***"****Por la cual se dictan disposiciones generales para la protección de datos personales"*
- Decreto 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"*
- Decreto 1078 de 2015 *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"*
- Decreto 415 de 2016 *"en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones"*
- Ordenanza departamental 430 de 2016 *"Política TIC que busca convertir al departamento en un territorio inteligente e innovador"*
- 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"*
- Norma Técnica Colombiana NTC-ISO/IEC 27001:2013 *"Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos"*
- Guía Técnica Colombiana GTC-ISO/IEC 27002 *"Tecnología de la información. Técnicas de seguridad. Código de Practica para Controles de Seguridad de la Información"*
- Norma Técnica Colombiana NTC-ISO 31000 *"Gestión del Riesgo. Directrices"*

El presente aparte deberá estar sometido a actualizaciones conforme se expidan o deroguen normatividades, decretos o cualquier otro lineamiento.

TERMINOS Y DEFINICIONES

A continuación, se presenta el significado a términos que serán de manejo del presente documento y en el desarrollo de Modelo de Seguridad y Privacidad de la Información (MSPI)

Activo: Es cualquier cosa que tiene valor para la organización. Existen varios tipos de activos como:

- Información.
- Software.
- Físicos o hardware.
- Servicios.
- Talento humano.
- Intangibles como la reputación y la imagen.

Amenaza: Causa potencial de un incidente no deseado, que pueda ocasionar daño a un sistema u organización.

Análisis de Impacto al Negocio: Donde se determinan los recursos críticos y el tiempo de recuperación con las respectivas ventanas de criticidad mediante las cuales se debe restaurar los activos evaluados.

Análisis del Riesgo: Uso sistemático de la información para identificar las fuentes y estimar el riesgo.

Confidencialidad: Aseguramiento de que la información es accesible sólo para quienes están autorizados.

Custodio: Encargado de guardar el activo con cuidado y vigilancia. Es una parte designada de la organización, un cargo, proceso, o grupo de trabajo encargado de administrar los componentes tecnológicos donde se encuentra la información (sea el caso que depende de componentes tecnológicos); además se encarga de hacer efectivos los controles de seguridad administrativos que el propietario de la información haya definido, tales como el manejo de archivos, el uso de copias y la eliminación.

Disponibilidad: Aseguramiento de que los usuarios autorizados tengan acceso a la información y sus recursos asociados cuando lo requieran.

Propietario: El término “Dueño” o “Propietario” identifica a un individuo o a una entidad que tiene responsabilidad aprobada por la Dirección por el control de la producción, el desarrollo, el

mantenimiento, el uso y la seguridad de los activos. El término “Propietario” no implica que la persona tenga realmente los derechos de propiedad de los activos.

Evento de Seguridad de la Información: Se refiere a cualquier situación que pueda afectar los niveles de riesgo, sin afectar de forma necesaria al negocio o a la información. Por ejemplo, una persona sospechosa que se encuentra cerca de un área protegida representa un incremento en el riesgo, pero no afecta los resultados comerciales ni compromete la información que se encuentre en el espacio restringido.

Incidente de Seguridad de la Información: Es un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones e información del negocio o ya se ha materializado y afectado a la organización.

Integridad: Salvaguarda de la exactitud y completitud de la información y sus métodos de procesamiento.

Principio del Mínimo Privilegio: Todos los usuarios en cualquier momento deben contar con tan pocos privilegios como sea posible para el ingreso a un activo de información.

Riesgo: Combinación de la probabilidad de un evento y sus consecuencias.

Seguridad de la Información: Preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio, trazabilidad y confiabilidad podrían estar involucradas.

POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Política General de Seguridad de la Información.

La Presidencia del Concejo Distrital de la Ciudad de Cali y la Oficina de Informática y Telemática, entendiendo la importancia de la adecuada gestión de la seguridad de la información en sus proceso, servicios y activos de información como uno de los habilitadores transversales de la Política de Gobierno Digital, la cual se encuentra alineada con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas, se ha comprometido con la implementación de un Modelo de Seguridad y Privacidad de la Información, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos y el estricto cumplimiento de las leyes y en concordancia con la misión y visión del Concejo.

Para el Concejo de Cali, la protección de la información busca salvaguardar los activos de información mediante la adopción de medidas que contribuyan a la disminución del impacto generado por la materialización de los riesgos, manteniendo un nivel de exposición tolerable respecto a la integridad, confidencialidad y la disponibilidad de los activos de Información.

De acuerdo con lo anterior, esta política aplica para el Concejo según como se defina en el alcance a sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del MSPI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los servidores públicos, ciudadanía y entidades del estado.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los servidores públicos, contratistas, terceros, proveedores, aprendices, practicantes y ciudadanía en general.
- Garantizar la continuidad del negocio frente a incidentes.

A continuación, se establecen 12 principios de seguridad que soportan el MSPI del Honorable Concejo de la Ciudad de Cali:

- El Concejo de Cali ha tomado la decisión definir, implementar, operar y mejorar de forma continua un Modelo de Seguridad y Privacidad de la Información, soportado en directrices claras alineados a las necesidades del negocio, y a los requerimientos regulatorios que apliquen.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los servidores públicos, contratistas, proveedores y/o terceros que intervengan dentro de los procesos misionales, estratégicos, apoyo y de control del Concejo de Cali.
- El Concejo de Cali protegerá la información generada, procesada o resguardada por los procesos de negocio, infraestructura tecnológica y activos de información, ante el riesgo por el uso y acceso incorrecto a los recursos de información por parte de servidores públicos, contratistas, proveedores y ciudadanos del común. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información.
- El Concejo de Cali velara por la protección de las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- El Concejo de Cali controlara la operación de sus procesos de negocio velando por la seguridad de los recursos tecnológicos y las redes de datos.
- El Concejo de Cali, implementara controles de acceso a la información, sistemas y recursos de red.
- El Concejo de Cali, velara para que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- El Concejo de Cali, velara por una mejora efectiva de su MSPI, a través de una adecuada gestión de los eventos, incidentes y debilidades de seguridad asociados a los sistemas de información y espacios físicos.
- El Concejo de Cali, velara la disponibilidad de sus procesos de negocio y la continuidad de sus operaciones basado en el impacto que puedan generar los incidentes de seguridad de la información.
- El Concejo de Cali, velara el cumplimiento de las obligaciones legales, regulatorias y contractuales, especialmente en las que intervenga el componente de seguridad de la información.
- El concejo de Cali velara por promulgar, incentivar y capacitar a servidores públicos, contratistas, proveedores y terceros en el uso de los activos de información de la institución como también en amenazas de índole informático.
- El concejo de Cali velara por el cuidado y seguridad perimetral de las instalaciones del Concejo y recintos de acceso restringido.

Deberes de los usuarios en el uso de los recursos de información

- Usar los activos de información del Concejo Distrital de Cali, solamente en pro de los objetivos del Concejo y según su contrato así lo determine para el ejercicio y cumplimiento de sus obligaciones laborales.
- Respetar la confidencialidad de los recursos de información del Concejo.
- No compartir perfiles de usuario, contraseñas, sesiones activas en equipos de cómputo, documentos confidenciales o cualquier otro tipo de recurso de información personal en el uso de sus actividades laborales.
- No dejar a la vista nombres de usuarios, contraseñas, llaves o cualquier otro elemento que posibilite el acceso a recursos de información del Concejo.
- Al momento de ausentarse de su estación de trabajo, realizarla el bloqueo de equipos de cómputo y retire de la vista documentos o cualquier otro recurso de información confidencial físico.
- Al momento de imprimir o escanear documentos estos deben de ser recogidos en la mayor brevedad de los equipos de impresión, evitando dejar información por largos periodos de tiempo en estos equipos, debido a que son de uso general de los empleados y se encuentran por lo general en espacios no restringidos.
- Una vez finalice su vínculo laboral con el Concejo Distrital de Cali, debe reintegrar en buen estado y no conservar ningún tipo de copia de los activos de información dados en el ejercicio de sus actividades laborales en el Concejo.
- Esta prohibido el uso de elementos de almacenamiento externos como memorias USB, discos duros extraíbles, Cd´s o cualquier otro medio de almacenamiento de información ajeno a los equipos de computo del Concejo. Se encuentran exentos de este punto procesos y/o procedimientos dependientes de dispositivos de almacenamiento externo para el cumplimiento de sus obligaciones laborales como lo son los procesos de copias de respaldo, los cuales se realizan en medios propios del Concejo.
- Esta estrictamente prohibida la divulgación, cambio o retiro no autorizado de activos de información fuera de las instalaciones del Concejo, sea el caso en el que por circunstancias de fuerza mayor o falta de espacio físico en las instalaciones del Concejo se requiera que los servidores públicos y/o contratistas deban desempeñar sus actividades desde sus casas este será notificado mediante comunicado formal por la presidencia del Concejo.
- Esta estrictamente prohibido el uso de software no licenciado en los recursos tecnológicos del Concejo, copiar software licenciado por el Concejo de Cali para el uso en equipos personales y/o entregarlo a terceros.
- Está prohibida la instalación de cualquier tipo de software no autorizado en los equipos de computo del Concejo Distrital de Cali, esta tarea es propia los funcionarios adscritos a la Oficina de Telemática y Informática del Concejo, de requerir el uso de software diferente al que tiene a

su disposición el Concejo, deberá elevar la solicitud de estudio y viabilidad a la Oficina de Telemática y Informática para su atención, es de aclarar que todo el software a ser usado en el Concejo debe estar completamente licenciado y su valor es asumido por la presidencia del Concejo o por la persona solicitante y se deberá aportar a la oficina de Telemática e Informática el correspondiente respaldo documental emitido por el fabricante por la adquisición de nuevo software.

- Cuando un usuario termine la relación laboral con el Concejo Distrital de Santiago de Cali, es responsabilidad de su superior inmediato avisar a la Oficina de Informática y Telemática para desactivación del correo y demás accesos a aplicaciones a las cuales se encuentre habilitado el usuario.
- No generar o enviar correos electrónicos a nombre de otra persona.
- No ejecutar ningún archivo contenido en un mensaje de correo no solicitado o enviado por un remitente desconocido. Dado el caso de recibir un correo sospechoso el servidor público, contratista y/o proveedor deberá informarlo inmediatamente a la Oficina de Informática y Telemática.
- La Oficina de Informática y Telemática es la encargada de autorizar el acceso a Internet de los equipos de los usuarios y de autorizar la creación de usuarios de correo electrónico institucional (nombre de usuario@concejodecali.gov.co). Si en determinado caso, el usuario quien tiene un correo corporativo se olvida o bloquea su contraseña, deberá informar por escrito al jefe de la Oficina de Informática y Telemática para su correspondiente desbloqueo, adicional es responsabilidad del usuario, el cambio de la clave inmediatamente haga el primer acceso luego de haberse desbloqueado su cuenta de correo.
- Es de uso obligatorio del correo electrónico institucional, para todo lo relacionado con las comunicaciones al interior del Concejo, su uso es personal e intransferible.
- Está prohibido el envió de correos masivos (Broadcast), por parte de usuarios diferentes al personal de comunicaciones, presidencia o cualquier otro usuario que así haya recibido autorización para poder hacerlo.

Deberes de los responsables del Personal

- Conceder a los empleados a su cargo la autorización de acceso a activos de información conforme a las actividades laborales que vaya a desempeñar.
- Realizar segregación de funciones al momento de asignar responsabilidades y acceso a recursos de información del Concejo, un usuario no debe tener permisos suficientes para desarrollar una actividad de principio a fin y sin la participación de una doble intervención como medida de control.
- Restringir el acceso del personal a áreas que hayan sido denominadas como restringidas.
- Ser el responsable de conocer, solicitar y ratificar los privilegios de acceso a los empleados bajo su direccionamiento.

- Conservar el registro con los empleados con privilegios de acceso sensibles. Adicional el área responsable de operar el MSPI, debe definir un tiempo en el cual se requiera ratificar por parte de los coordinadores y/o jefes los privilegios de acceso sensible del talento humano bajo su cargo, y mantener actualizadas las autorizaciones y perfiles de usuario tomando como base el listado de empleados activos de Recursos Humanos, para tener como referencia el área a la que pertenece cada uno.
- Los contratos de prestación de servicios, obra labor o cualquier otro tipo de contratación outsourcing, deben detallar dentro del cuerpo del contrato los acuerdos de propiedad de la información y la no divulgación de información clasificada como confidencial.
- Se debe determinar el tiempo máximo en el que dado el caso en el que un empleado se asenté de sus labores, se deban suspender sus privilegios de acceso a áreas restringidas, sistemas de información e información confidencial.
- Dado el tiempo máximo ante la ausencia de un empleado de sus funciones, el superior inmediato debe:
    - Notificar al área encargada del retiro de privilegios a áreas restringidas, sistemas e información del empleado ausente.
    - Notificar la fecha desde la cual se deben suspender los privilegios.
- Cuando un empleado se aparte de sus labores por voluntad propia o por disposición de estamentos superiores, el jefe inmediato es responsable por:
    - Solicitar la revocación de las autorizaciones y perfiles de acceso a los sistemas de información del Concejo de Cali.
    - Dado el caso en que se requiera, revocar o restringir primero los privilegios de acceso a áreas restringidas y sistemas de información antes de notificar al empleado su desvinculación de sus labores.
    - Recoger el equipo de cómputo, elementos de acceso a zonas restringidas como tarjetas de proximidad o llaves, documentos y demás elementos dados en encargo al empleado a desvincularse.

Directrices Relacionados con el Manejo de Información Confidencial.

- Los documentos en los cuales repose información con este tipo de característica no pueden ser dejados desatendidos o inseguros.
- Debe encontrarse etiquetado de tal manera que sea identificable para los usuarios que se trata de un documento que requiere suma atención y cuidado.
- Se debe dar a conocer a los empleados la clasificación en el etiquetado de la información para que estos puedan dar el respectivo cuidado a la información.
- Reuniones relacionadas con el manejo de información confidencial deben ser llevadas a cabo en áreas cerradas, como oficinas, salas de juntas o cualquier otro espacio cerrado pertinente para dicha acción.

- No se debe enviar información confidencial a través de medios que no cuenten con el aval de la oficina de Telemática e Informática de Concejo de Cali, como lo son teléfonos celulares, aplicaciones de mensajería como Whatsapp o redes sociales.
- El acceso o distribución de información de uso interno debe estar limitado solamente a servidores públicos, empleados u otros con la necesidad de conocerla o usarla para el cumplimiento estricto de sus funciones.
- Cada vez que se requiera imprimir o escanear un documento de índole confidencial o de circulación limitada o restringida, deben de ser impresos o escaneados en áreas seguras o bajo supervisión.
- Los mecanismos usados en la distribución de la información, deben contemplar confirmación de recibido.
- Los lineamientos en el manejo de información confidencial aplican para documentos originales como para copias controladas de los mismos.
- La información confidencial en medio físico como papel, debe ser almacenada en archivos bajo llave o espacios físicos con medidas de seguridad como candados o puertas de proximidad que permitan controlar su acceso.
- Se debe generar una ventana de revisión aleatoria sobre los documentos almacenados en los espacios seguros a fin de revisar su condición físico ambientales y comprobar que sigan siendo legibles.
- Dado casos de fuerza mayor como situaciones de pandemia o algún otro suceso que obligue a trabajar fuera de las instalaciones del Concejo Distrital de la Ciudad de Cali, las personas que tienen acceso a la información son responsables por la seguridad de la misma y velar porque las medidas de seguridad sean lo mas fieles posibles a con las que se trata la información al interior de las instalaciones del Concejo.

Políticas de Respaldo, Custodia y Recuperación de Información

- El Concejo Distrital de Cali, dispone de la transmisión de correos electrónicos bajo el servicio de mensajería electrónica de Google, quien provee el dominio “Concejodecali.gov.co” y 15 GB de almacenamiento en la Nube (Google Drive) para el almacenamiento de información propia de la actividad laboral de los Servidores Públicos, Contratistas o Proveedores a quien se haya otorgado una cuenta de correo electrónico del Concejo y unidades compartidas por cada uno de los procesos adscritos al Concejo Distrital con una capacidad de almacenamiento ilimitado, teniendo en cuenta las herramientas de las que dispone el Concejo se recomienda, que dado el caso en el que un Servidor Público, Contratistas o Proveedores requiera realizar el respaldo de información de uso laboral, lo realicen a través de Google Drive.
- Cada administrador de sistemas de información del Concejo es el responsable de realizar el respaldo de la información de los equipos que funcionan como servidores a su cargo y que adicional contengan las bases de datos de los aplicativos que en ellos se encuentran alojados.

Se debe definir por parte del administrador del sistema la periodicidad (diaria, semanal, mensual o cual sea considerada por el administrador como pertinente) con la que será realizada la actividad de respaldo de información teniendo en cuenta la importancia y criticidad de la información a respaldar.

- La Información de respaldo de servidores deberá ser almacenada en un equipo de Cómputo o servidor diferente al cual se está realizando el respaldo o en dispositivos de almacenamiento externo para el uso exclusivo de resguardar información de respaldo, estos últimos deberán estar resguardados en lugares seguros con acceso limitado preferiblemente solo a la persona encargada de realizar la actividad de respaldo de información.
- Es responsabilidad de cada usuario, velar por tener el respaldo de su información y definir la periodicidad con la que realizara dicha actividad.
- Se recomienda que el almacenamiento de los Backups almacenados en disco duros, cintas o cualquier otro elemento físico, sea almacenado en espacios diferentes a donde reside la información primaria. De este modo se evita la pérdida dado que se presenten situaciones que afecten la infraestructura física del Concejo Distrital de Cali.
- El Jefe de la Oficina de Telemática e Informática deberá velar por el uso de antivirus en los equipos de cómputo del Concejo.
- Los usuarios responsables de realizar el respaldo de la información, también son responsables de restaurarla dado situaciones que así lo ameriten.
- Todos los medios que contengan información clasificada, restringida o confidencial una vez finalicen el ciclo de vida para el cual fueron concebidos deberán ser sobrescritos, realizar un borrado magnético o destruidos físicamente a fin de asegurar que la información que almacenaban no será accedida por personas a las cuales la información no debía estar disponible.
- Dado el caso en el que la actividad de respaldo de información sea contratada con un tercero se deberá asegurar que en el contrato que se suscriba con esa parte, se estipulen clausulas que impiden la divulgación de la información que es objeto de respaldo, como también penalidades dado el caso de ocurrir situaciones que comprometan la confidencialidad, disponibilidad e integridad de la información, como también debe quedar claro que toda la información respaldada es propiedad del Concejo Distrital de Santiago de Cali y una vez finalizado el contrato entre las partes esta será reintegrada al Concejo y la parte con la que se realizo el contrato no quedara con ningún tipo de copia.

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.