CONCEJO
SANTIAGO DE CALI

OFICINA INFORMÁTICA

INSTRUCTIVO POLITICA DE SEGURIDAD DE LA INFORMACIÓN

SANTIAGO DE CALI, SEPTIEMBRE DEL 2020

CONTENIDO

1. OBJETIVO

El propósito de este documento es definir la política administrativa y proveer una guía respecto al uso responsable de los Sistemas de Información del Concejo Distrital de Santiago de Cali. En este orden de ideas, hay que comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos y bienes, sus elementos de seguridad y la responsabilidad al buen uso que le den los funcionarios del Concejo.

Es importante señalar que las políticas por sí solas no constituyen una garantía para la Seguridad del Concejo, es un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con el Concejo.

En este documento se trata de plasmar el enfoque de la norma ISO 27001 la cual comprende la política, estructura organizativa, procedimientos, procesos y recursos necesarios para implantar la gestión de la seguridad de la información.

Un SGSI se implanta de acuerdo a estándares de seguridad como el ISO 27001 basado en el código de buenas prácticas y objetivos de control ISO 17799, el cual se centra en la preservación de las características de **CONFIDENCIALIDAD**, **INTEGRIDAD** Y **DISPONIBILIDAD**, sobre el Sistema de Gestión de Seguridad de la Información, pero para darle mayor profundidad y precisión, es necesario contratar una auditoria externa, por personal altamente calificado y certificado en seguridad informática.

2. ALCANCE

Las políticas definidas en el presente documento aplican a todos los Servidores Públicos del Concejo Distrital de Santiago de Cali, que hagan uso de los diferentes Sistemas de Información (Aplicativos) o Bases de Datos.

3. DEFINICIONES

ACTIVO**:** Se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

ARCHIVO ELECTRONICO: Conjunto de documentos electrónicos, producidos y tratados archivísticamente, siguiendo la estructura orgánico funcional del productor, acumulados en un proceso natural, por una institución en el transcurso de su gestión.

BACKUP: guardar en un medio extraíble (para poder guardarlo en lugar seguro) la información sensible referida a un sistema. Es una copia de seguridad de los datos. Se recomienda hacer esta labor periódicamente.

BASE DE DATOS: Conjunto de datos que pertenecen al mismo contexto almacenados sistemáticamente para su posterior uso.

CALIDAD. Grado en el que un conjunto de características inherentes cumple con los requisitos.

CLIENTE. Organización, entidad o persona que recibe un producto y/o servicio. El término cliente incluye a los destinatarios, usuarios o beneficiarios (DUB); los cuales pueden ser internos o externos al Concejo.

CONFIDENCIALIDAD**:** Acceso a la información por parte únicamente de quienes estén autorizados.

CONTROL: Capacidad de ejercer o dirigir una influencia sobre una situación dada o hecho. Es una acción tomada para hacer un hecho conforme a un plan. Se concibe como la verificación a posteriori de los resultados conseguidos en el seguimiento de los objetivos planteados.

DECISIÓN: Elección de un curso de acción determinado entre varios posibles.

DISPONIBILIDAD**:** Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

DOCUMENTO. Información y su medio de soporte.
Ejemplo: Formato, especificación, procedimiento documentado, dibujo, informe, norma. Su medio de soporte puede ser papel, magnético, óptico o electrónico, muestra patrón o una combinación de estos.

ESTRATEGIA: Conjunto de decisiones que se toman para determinar políticas, metas y programas.

HARDWARE: Conjunto de los componentes que integran la parte material de un computador. Es la parte física, lo que se puede tocar.

INFORMACIÓN. Puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

INTEGRIDAD: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

MATERIAL NO PERMITIDO. Incluye la transmisión, distribución o almacenamiento de todo material que viole cualquier ley aplicable. Se incluye sin limitación, material protegido por derechos de reproducción, marca comercial, secreto comercial, u otro derecho sobre la propiedad intelectual utilizada sin la debida autorización y material que resulte obsceno, difamatorio o ilegal bajo las leyes nacionales.

MECI. Modelo Estándar de Control Interno para el Estado Colombiano Proporciona la estructura básica para evaluar la estrategia, la gestión y los propios mecanismos de evaluación del proceso administrativo, y aunque promueve una estructura uniforme, se adapta a las necesidades específicas de cada entidad, a sus objetivos, estructura, tamaño, procesos y servicios que suministran.

META: objetivo cuantificado a valores predeterminados.

MODELO OPERATIVO POR PROCESOS. Metodología mediante la cual se desarrolla el Modelo Gerencial fundamentado en el Modelo Estándar de Control Interno MECI.

NORMA: Forma en que realiza un procedimiento o proceso

PARTE INTERESADA. Organización, persona o grupo que tenga un interés en el desempeño de una entidad. Ejemplo: Beneficiarios, servidores públicos y/o particulares que ejercen funciones públicas de una entidad, proveedores, sindicatos, entidades de control, veedurías ciudadanas o la sociedad en general.

PLAN: Conjunto de decisiones que definen cursos de acción futuros y los medios para conseguirlos. Consiste en diseñar un futuro deseado y la búsqueda del modo de conseguirlo.

PLATAFORMA TECNOLOGICA. Conjunto de elementos de Hardware y Software que sirven de base para el desarrollo y funcionamiento de los Sistemas de Información.

POLÍTICA. Es una actividad orientada en forma ideológica a la toma de decisiones de un grupo para alcanzar ciertos objetivos. También puede definirse como el ejercicio del poder para la resolución de un conflicto de intereses.

PROCEDIMIENTO: Definición detallada de pasos a ejecutar para desarrollar una actividad determinada. Se debe definir quién hace qué, dónde, cuándo, porqué y cómo.

PROCESO. Conjunto de actividades relacionadas mutuamente o que interactúan para generar valor y las cuales transforman elementos de entrada en resultados.

PRODUCTO. Resultado de un proceso o un conjunto de procesos.

PRONOSTICO: predicción del comportamiento futuro, con el agregado de hechos concretos y conocidos que se prevé influirán en los acontecimientos futuros

PROGRAMA: Secuencia de acciones interrelacionadas y ordenadas en el tiempo que se utilizan para coordinar y controlar operaciones.

PROVEEDOR. Organización o persona que proporciona un producto y/o servicio. Puede ser interno o externo.

PROYECCIÓN: predicción del comportamiento futuro, basándose en el pasado sin el agregado de apreciaciones subjetivas.

RECURSO INFORMÁTICO. Elementos informáticos (base de datos, sistemas operacionales, redes, sistemas de información y comunicaciones) que facilitan servicios informáticos.

REDES. Incluye varios sistemas electrónicos como redes de video, datos, voz y dispositivos de almacenamiento.

ROL. Es un conjunto de permisos que puede asignarse a un usuario que se registra en un administrador de sistemas. Normalmente, los roles se definen de modo que incluyan permisos que guarden cierta relación y suelen corresponderse con algún rol de la vida real.

RIESGO: proximidad o posibilidad de un daño, peligro. Cada uno de los imprevistos, hechos desafortunados, etc., que puede tener un efecto adverso. Sinónimos: amenaza, contingencia, emergencia, urgencia, apuro.

SISTEMA. Tradicionalmente un Sistema es entendido como la interrelación mutua que se establece entre los elementos que componen un todo y que conducen al logro de objetivos.

SISTEMA DE CONTROL INTERNO. Se entiende por control interno el sistema integrado por el esquema de organización y el conjunto de los planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por una entidad, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales y legales vigentes.

SISTEMA DE DESARROLLO ADMINISTRATIVO. Es el conjunto de políticas, estrategias, metodologías, técnicas y mecanismos de carácter administrativo y organizacional para la gestión y manejo de los recursos humanos, técnicos, materiales, físicos y financieros, orientado a fortalecer la capacidad administrativa y el desempeño institucional.

SISTEMAS DE INFORMACIÓN Incluye cualquier sistema físico o aplicación de software que sea administrado por la Institución y por los cuales ella sea responsable, como computadores, redes, servidores, enrutadores y aparatos

similares junto con sus aplicaciones de red o aplicaciones de escritorio como sistemas operativos, aplicaciones de Internet etc.

SISTEMAS DE GESTIÓN. Es el conjunto de actividades que, interrelacionadas y a través de acciones específicas, permiten definir e implementar los lineamientos generales y de operación de las entidades públicas.

SISTEMA DE GESTIÓN DE LA CALIDAD. Herramienta de gestión sistemática y transparente que permite dirigir y evaluar el desempeño, en términos de calidad y satisfacción social en la prestación de los servicios. Está enmarcado en los planes estratégicos y de desarrollo.

SOFTWARE: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en un computador.

USO INDEBIDO. Actividad o comportamiento conocida como mala o inapropiada.

USUARIOS INTERNOS. Todas aquellas personas naturales que tienen algún tipo de vinculación contractual o de prestación de servicios con el Concejo Distrital de Santiago de Cali, que deban tener acceso a Recursos Informáticos.

4. CONTENIDO Y DESARROLLO

El acceso a los Sistemas de Información en el Concejo Distrital de Santiago de Cali, es un privilegio y no un derecho, y debe ser tratado de esta manera por todos los usuarios de dichos sistemas.

Deberes de todos los usuarios.

- Actuar honesta y responsablemente.
- Cada usuario es responsable por la integridad de las instalaciones físicas y sus métodos de control.
- Respetar los derechos de otros usuarios.
- Respetar toda licencia pertinente y acuerdo contractual que esté relacionado con los sistemas de información del Concejo.
- Actuar de acuerdo con los lineamientos expuestos en estas políticas, las normas y Leyes Nacionales pertinentes.

El incumplimiento de esta política puede resultar en la negación de acceso a los sistemas de información del Concejo.

- Cambiar la configuración de los Sistemas de cómputo o instalar cualquier tipo de software.
- Instalar software que no tenga licencia en el Concejo. Cualquier tipo de instalación que se necesite, debe hacerla la Oficina de Informática y Telemática.
- Violar cualquier licencia de software o derechos de autor, incluyendo la copia o distribución de software protegido legalmente, sin la autorización escrita del propietario del software.
- Usar las comunicaciones electrónicas para violar los derechos de propiedad de los autores.
- Descargar o publicar material ilegal, con derechos de propiedad o material nocivo, usando un computador del Concejo, así esté dirigido a nombre personal.
- Transportar o almacenar material con derechos de propiedad o material nocivo, usando las redes del Concejo.
- Lanzar cualquier tipo de virus, gusano, o programa de computador cuya intención sea hostil o destructiva.
- Enviar cualquier comunicación electrónica fraudulenta.
- Violar cualquier ley o regulación nacional respecto al uso de sistemas de información.
- Usar las comunicaciones electrónicas para dañar o perjudicar de alguna

manera los recursos disponibles electrónicamente.

- Interferir sin autorización, el acceso a otros usuarios a los recursos de los sistemas de información.
- Transgredir o burlar las verificaciones de identidad u otros sistemas de seguridad.
- Permitir que personas ajenas a la organización manipulen los sistemas de cómputo, sólo los Líderes Funcionales podrán autorizar que los equipos de su área sean utilizados por terceros.
- Mutilar físicamente, alterar o extraviar el contenido o información de expedientes físicos y electrónicos.
- Interferir sin autorización el acceso a otros usuarios a los recursos de los sistemas de información.
- Utilizar los sistemas de información para propósitos ilegales o no autorizados.

POLÍTICAS DE CORREO ELECTRÓNICO

El correo electrónico debe usarse de manera profesional y cuidadosa dada su facilidad de envío y redirección. Los usuarios deben ser especialmente cuidadosos con los destinatarios colectivos y los foros de discusión.

Cuando termine la relación laboral con el Concejo Distrital Santiago de Cali, es responsabilidad de su superior inmediato avisar a la Oficina de Informática y Telemática para desactivación de ese correo.

No generar o enviar correos electrónicos a nombre de otra persona sin su autorización o suplantándola.

No ejecutar ningún archivo contenido en un mensaje de correo no solicitado o enviado por un remitente desconocido. Mucho menos si estos archivos tienen doble extensión. 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 y se le olvida o bloquea su contraseña, deberá informar por escrito al jefe de la Oficina de Informática y Telemática para su correspondiente desbloqueo y es responsabilidad del usuario su cambio de clave inmediatamente.

Obligatorio el uso de los correos electrónicos institucionales, para todo lo relacionado con las labores internas del Concejo y su uso es personal no podrán mas de 1 persona utilizar el mismo correo.

POLITICAS DE ACCESO A LOS SISTEMAS DE INFORMACIÓN.

USO PERMITIDO.

Los sistemas de información del Concejo son primordialmente para uso de asuntos relacionados con la misma. Los sistemas de información pueden ser usados para asuntos personales siempre y cuando su utilización esté de acuerdo con estas políticas y no interfiera con las operaciones de la institución o con las tareas de los demás usuarios. Bajo ninguna circunstancia el uso personal de estos sistemas por parte de los usuarios del Concejo, debe influir de manera negativa en el desempeño de las tareas y responsabilidades para con la Institución. El uso personal puede ser negado en casos en los que se haga uso excesivo de los recursos de los sistemas de información.

ACCESO.

Está prohibido el acceso no autorizado a los sistemas de información del Concejo. Nadie debe usar la identificación, identidad o contraseña de otro usuario, y de la misma manera ninguno debe dar a conocer su contraseña o identificación, excepto en casos que faciliten la reparación o el mantenimiento de un equipo de cómputo, para el ingreso al mismo, pero de ninguna manera claves de aplicativos. Si en determinado caso, el usuario quien tiene acceso a un aplicativo en particular y se le olvida o bloquea su contraseña, deberá informar por escrito al jefe de la Oficina de Informática y Telemática para su correspondiente desbloqueo y es responsabilidad del usuario su cambio de clave inmediatamente.

Cuando un usuario termina su relación laboral o contractual con la con el Concejo, sus identificaciones y contraseñas deben ser entregadas a su jefe inmediato, para que este formalmente la comunique por escrito a la Oficina de Informática y Telemática, para la eliminación de su nombre de usuario y contraseña.

POLÍTICAS DE USO INDEBIDO DE COMPUTADORES Y REDES.

La siguiente lista intenta brindar una referencia de las actividades que se ajustan a la categoría de uso inadecuado para “sistemas y redes”, y para “correo electrónico y sistemas de comunicaciones”:

- Intentar modificar equipos de cómputo, Software, Información o periféricos sin la debida autorización.
- Trasladar equipos entre áreas o fuera de la oficina, sin la debida autorización del responsable del Almacén del Concejo y la Jefe de Recurso Físico.

- Cambiar la configuración de los Sistemas de cómputo o instalar cualquier tipo de software.
- Instalar software que no tenga licencia en el Concejo. Cualquier tipo de instalación que se necesite, debe hacerla la Oficina de Informática y Telemática.
- Violar cualquier licencia de software o derechos de autor, incluyendo la copia o distribución de software protegido legalmente, sin la autorización escrita del propietario del software.
- Usar las comunicaciones electrónicas para violar los derechos de propiedad de los autores.
- Descargar o publicar material ilegal, con derechos de propiedad o material nocivo, usando un computador del Concejo, así esté dirigido a nombre personal.
- Transportar o almacenar material con derechos de propiedad o material nocivo, usando las redes del Concejo.
- Lanzar cualquier tipo de virus, gusano, o programa de computador cuya intención sea hostil o destructiva.
- Enviar cualquier comunicación electrónica fraudulenta.
- Violar cualquier ley o regulación nacional respecto al uso de sistemas de información.
- Usar las comunicaciones electrónicas para dañar o perjudicar de alguna manera los recursos disponibles electrónicamente.
- Interferir sin autorización, el acceso a otros usuarios a los recursos de los sistemas de información.
- Transgredir o burlar las verificaciones de identidad u otros sistemas de seguridad.
- Permitir que personas ajenas a la organización manipulen los sistemas de cómputo, sólo los Líderes Funcionales podrán autorizar que los equipos de su área sean utilizados por terceros.
- Mutilar físicamente, alterar o extraviar el contenido o información de expedientes físicos y electrónicos.
- Interferir sin autorización el acceso a otros usuarios a los recursos de los sistemas de información.
- Utilizar los sistemas de información para propósitos ilegales o no autorizados.

4.1.4. POLÍTICAS DE CORREO ELECTRÓNICO

- El correo electrónico debe usarse de manera profesional y cuidadosa dada su facilidad de envío y redirección. Los usuarios deben ser especialmente cuidadosos con los destinatarios colectivos y los foros de discusión.
- Cuando un funcionario termine su relación laboral con el Concejo Distrital Santiago de Cali, es responsabilidad de su superior inmediato avisar a la Oficina de Informática y Telemática para desactivación de ese correo.
- No generar o enviar correos electrónicos a nombre de otra persona sin su autorización o suplantándola.
- No ejecutar ningún archivo contenido en un mensaje de correo no solicitado o enviado por un remitente desconocido. Mucho menos si estos archivos tienen doble extensión.
- 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 y se le olvida o bloquea su contraseña, deberá informar por escrito al jefe de la Oficina de Informática y Telemática para su correspondiente desbloqueo y es responsabilidad del usuario su cambio de clave inmediatamente.
- Es obligatorio el uso de los correos electrónicos institucionales, para todo lo relacionado con las labores internas del Concejo y su uso es personal no podrán mas de 1 persona utilizar el mismo correo.

4.1.5 POLÍTICAS DE RESPALDO (Backups).

- El administrador del sistema es el responsable de realizar el respaldo de la información de los equipos que funcionan como servidores del Concejo y que contenga la Base de Datos de los aplicativos. Por lo menos debe ser mensual.

- La información respaldada del Servidor deberá ser almacenada en el Disco Duro del Servidor, en un equipo de Cómputo y adicionalmente en otro sistema de almacenamiento (Memorias, Disco Duro Externo o

similar), procurando en lo posible, tener estas copias en un lugar diferente al sitio de trabajo o bajo llave.

- Es responsabilidad de cada usuario o líder de cada uno de los Procesos, velar por tener resguardada su información.

El Concejo cuenta actualmente con Correo corporativo bajo plataforma Google los cuales permiten usa la herramienta Google Drive para almacenamiento con capacidad de 15 Gigas, se recomienda usarla. Debido a que el Concejo no cuenta con sistemas más robustos para almacenamiento con sistemas espejos, hasta que no se adecue tecnológicamente el Concejo, para los procesos, procedimientos que requieran un almacenamiento mayor, hace necesario el uso alternativo de backups, de la información relevante, por algún medio como son:

- Medios Magnéticos y/o ópticos (Cds, Dvds, Memorias, etc).

Otra Recomentaciones:

- Se recomienda que el almacenamiento de los Backups realizarlos en sitios diferentes de donde reside la información primaria. De este modo se evita la pérdida si el desastre alcanza todo el edificio o local.

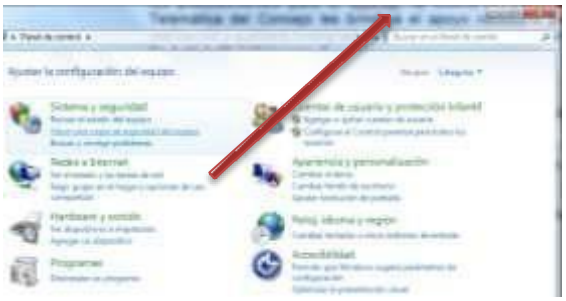
- La periodicidad de los respaldos (backup), dependerá de que cada líder de proceso priorice su información relevante, por ejemplo en archivos que sean de prioridad alta, se recomienda realizar el backup diario y en lo posible en medios duplicados ejemplo cd y en la nube, memoria y nube, etc; y en prioridad media se recomienda semanal su copia y en prioridad baja su recomendación es mensual, pero cada líder de proceso, de acuerdo a sus criterios, realizará la respectiva labor. Las prioridades van de acuerdo a la información misional o la información que produce cada proceso, éstas serías altas y medias y la prioridad baja son documentos alternos o personales que no hacen parte de cada uno de los procesos.

- Si algún Funcionario del Concejo tiene dudas de cómo realizar los procedimientos para el Backup, la oficina de informática y Telemática del Concejo les brindará el apoyo necesario para su realización y quedará consignado en el formato de atención a usuarios formulario web.

PASOS PARA LA REALIZACION DE BACKUPS EN SISTEMAS OPERATIVOS WINDOWS

Para la realización de la copia de Seguridad o Backup siga estas recomendaciones:

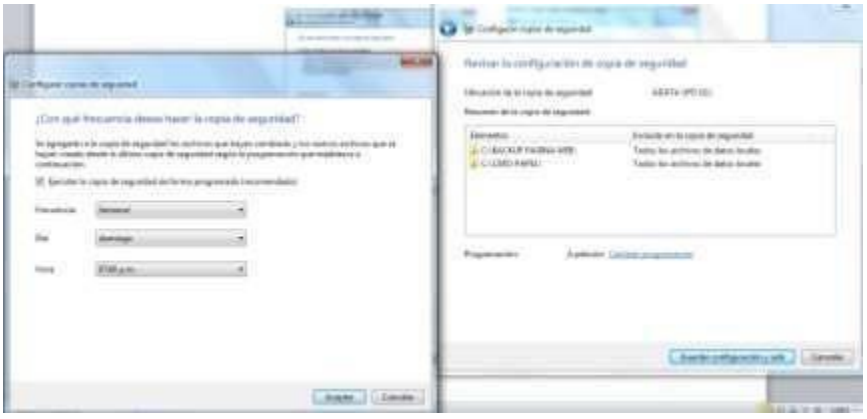
➢ Inicio/ Panel de Control/ Sistema y Seguridad/ Hacer una Copia de seguridad del Equipo.



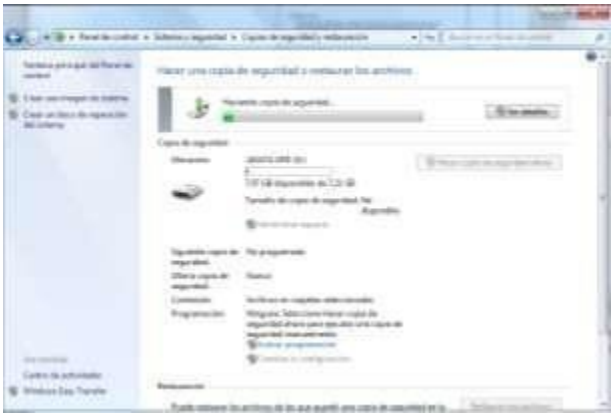
 Si no está configurado, dar click en configurar copias de seguridad

 Salen dos opciones, click en Dejarme elegir para configurar datos relevantes.

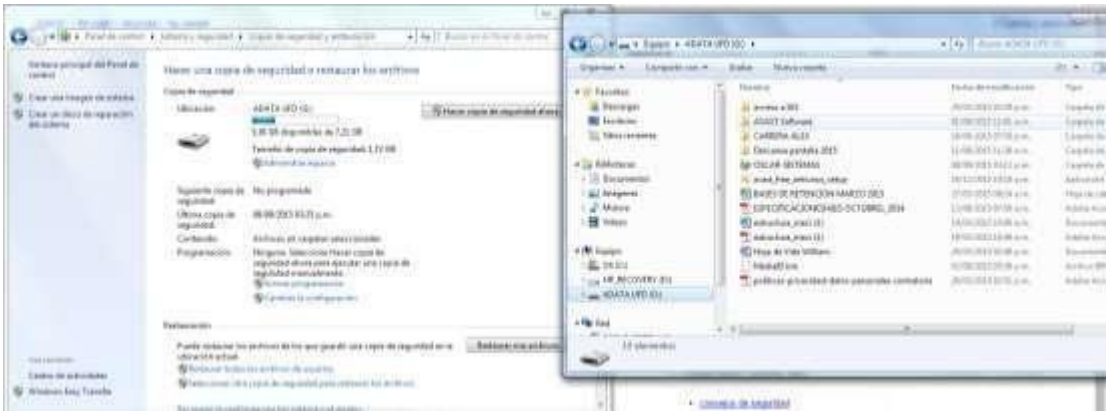
➢ Selecciona las carpetas contenedoras de los archivos a los cuales le quiere hace el Backup y click en siguiente.



 Si quiere ejecutar la copia programada, dar click y elegir la frecuencia, el día y la hora, si lo requiere manual solamente es quitar la selección.

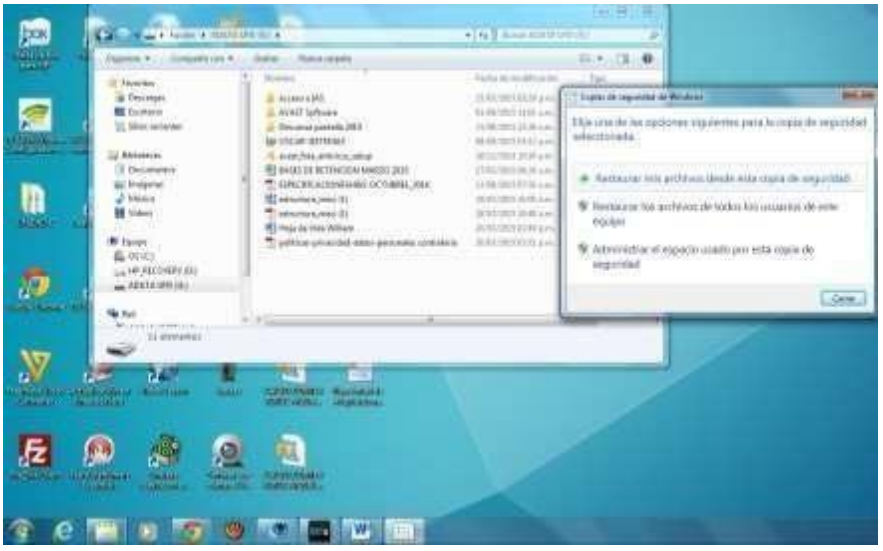


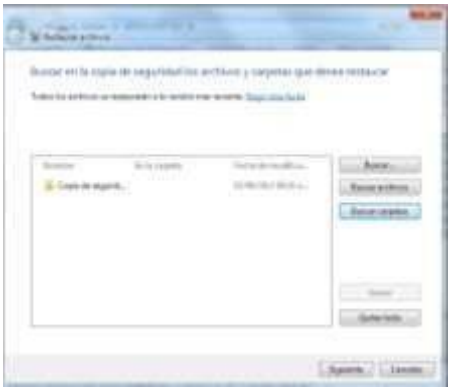
- Guardar configuración y salir.



PASOS PARA LA RESTAURACION DE BACKUPS O COPIAS DE SEGURIDAD EN SISTEMAS OPERATIVOS WINDOWS

- Desde explorador de Windows, seleccionar la ubicación donde tiene el Backup y dar click y después Restaurar mis archivos desde esta copia de seguridad.





➢ Direccionar donde quiere guardar la información de la restauración del Backup y listo.

PRECAUCIONES EN BACKUPS REALIZADOS EN CD O DVD

Se debe evitar tomar los discos apoyando los dedos sobre la superficie grabable. La forma correcta es tomarlo por los bordes o bien por el orificio central, para evitar de dejar impregnadas las huellas de los dedos, y por ende la acumulación de humedad.

Se deben utilizar sobres y fundas protectoras para guardar los discos, y cuando lo manipulamos, su forma correcta es dejar siempre hacia arriba la superficie de grabación.

Se deben almacenar en algún lugar donde no reciban excesivo calor o cambios bruscos de temperatura, como así también evitar la acumulación de polvo en el sitio donde colocamos nuestros discos y en lo posible se recomienda colocarlos en forma vertical.

No debe escribirse nada directamente sobre el disco, ya que los químicos que contienen los marcadores harán que la lámina superior se dañe, causando pérdida de la información grabada. Lo mejor es escribir directamente en el sobre o caja que contiene al disco, o bien adjuntar un papel con las anotaciones necesarias.

También se debe evitar el uso de etiquetas autoadhesivas ya que pueden producir los mismos efectos que los marcadores.

Se debe realizar, en los audios de las comisiones y/o plenarias, como se dijo anteriormente en las recomendaciones, tener un segundo duplicado, ya sea en disco duro externo, pc, en la nube o inclusive por los tamaños de los audios en cd, poderlos compilar varios en un DVD.

El procedimiento que se debe seguir para la grabación de los audios es, una vez terminada la sesión de la comisión y/o plenaria, el operario de sonido o quien haga sus veces grabará un CD o en algún otro medio informático, conteniendo el audio de la comisión y/o plenaria respectiva y lo pasará a la Secretaría General y/o Subsecretaría de acuerdo a la sesión correspondiente para que ellos custodien la información y realicen alternadamente un Backup de las sesiones en un medio externo (Disco duro externo, pc, nube, etc.) y a su vez el operario de sonido tendrá otra copia en un medio externo (Disco duro externo, pc, nube, etc.), como plan B por si algo pudiera ocurrir.

Para la custodia de los CDs o DVDs, debe seguirse el tema que habla de:

GOOGLE DRIVE ILIMITADO.

La Oficina de Informática y Telemática cuenta con la administración de una cuenta Google ilimitada bajo el dominio cali.gov.co la cual se utilizara de respaldo de la información crítica del Concejo Distrital de Santiago de Cali, Configurando Unidades Compartidas las cuales serán espacios utilizados por los procesos responsables de esta información y quienes serán los que alimenten y tengan acceso a ella, el jefe de Informática y Telemática tendrá un rol administración de la cuenta por ende tiene la responsabilidad de administrar todas las unidades compartidas tendrá acceso pero no podrá modificar ningún dato suministrado por los procesos.

SISTEMAS DE INFORMACION

Los sistemas de información que son administrados por empresas externas deben tener en los contratos la Confidencialidad, Disponibilidad e Integridad de los datos de la base de datos, además proporcionar sistemas de respaldo de información periódicos garantizando que el Concejo Distrital tenga a disposición la información cuando lo requiera.

4.1.6 Privacidad.

4.1.6.1 La privacidad de los usuarios no está garantizada. Cuando los Sistemas de Información del Concejo Distrital de Santiago de Cali funcionan correctamente, un usuario puede considerar los datos que genere como información privada, a menos que el autor de los datos realice alguna acción para revelarlo a otros. Los usuarios deben estar conscientes, sin embargo, de que ningún sistema de información es completamente seguro, que personas dentro y fuera de la institución pueden encontrar formas de tener acceso a la información. De acuerdo con esto, el Concejo implementara todos los recursos, herramientas y acciones encaminadas a proveer un entorno de privacidad de los sistemas de información, pero no puede, y no garantiza la privacidad de la información de los usuarios, quienes deben estar conscientes de ello permanentemente.

4.1.6.2 Reparación y mantenimiento de equipos. Periódicamente y por medio de un comunicado oficial, el personal de la Oficina de Informática y Telemática del Concejo, tienen la autoridad para acceder a archivos individuales o datos cada vez que deban realizar un mantenimiento, reparación o chequeo de equipos de computación. Sin embargo, el personal técnico no puede exceder su autoridad en ninguna de estas eventualidades para usar esta información para propósitos diferentes a los de mantenimiento o reparación. Cuando por alguna causa hubiera necesidad de formatear el equipo, es responsabilidad del usuario, realizar el Backup correspondiente de los datos.

4.1.6.3 Respuesta al uso indebido de Computadores y Sistemas de Información. Cuando por alguna causa razonable determinada por el funcionario responsable del proceso o el personal técnico de la Oficina de Informática y Telemática o quien haga sus veces, se cree que algún tipo de uso indebido se ha presentado como se describe en el numeral 4.1.3 de este documento, el Concejo con su personal técnico puede acceder cualquier cuenta, datos, archivos, o servicio de información perteneciente a los involucrados en el incidente, para investigar y aplicar las sanciones correspondientes.

4.1.7 Portal Web. El ordenador del gasto velará para que el Concejo tenga una página web activa oficial (www.concejodecali.gov.co). Los funcionarios de la oficina de Informáticay Telemática serán los encargados de su administración.

Los estándares para los contenidos considerados como oficiales del Concejo Distrital de Santiago de Cali, serán establecidos por el funcionario responsable del proceso adscrito a la Oficina de Comunicaciones y relaciones Corporativas, el Secretario General del Concejo Distrital y el acompañamiento de la Oficina de Informática y Telemática en los temas referentes a Gobierno Digital.

4.2 POLITICAS DE SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN.

4.2.1 Administrador de usuarios. Establece cómo deben ser utilizadas las claves de ingreso a los Sistemas de información del Concejo Distrital. Establece parámetros sobre la longitud mínima de las contraseñas, la frecuencia con la que los usuarios deben cambiar su contraseña y los períodos de vigencia de las mismas, entre otras.

4.2.2 Rol de Usuario. Los Sistemas de Información del Concejo Distrital de Santiago de Cali, deberán contar con un módulo que permita definir roles, definiendo las acciones permitidas por cada uno de estos; permitir la asignación a cada usuario de posibles y diferentes roles y permitir un rol de usuario para la administración de los mismos. Estos roles o perfiles, deberán estar por escrito, con el visto bueno del Jefe Responsable del o de los aplicativos y ser validados por los usuarios responsables del mismo.

CONCEJO SANTIAGO DE CALI	INSTRUCTIVO POLITICAS DE SEGURIDAD INFORMÁTICA			ISO 9001:2015 BUREAU VERITAS Certification Nº CO18.03305
	CÓDIGO: 21.3.23.5.15.278	**FECHA DE APROBACIÓN:**	SISTEMA DE GESTIÓN DE LA CALIDAD CONCEJO MUNICIPAL DE SANTIAGO DE CALI	
	VERSIÓN: 06	**09-09-2020**		

CONCEJO SANTIAGO DE CALI	INSTRUCTIVO POLITICAS DE SEGURIDAD INFORMÁTICA			ISO 9001:2015 BUREAU VERITAS Certification Nº CO18.03305
	CÓDIGO: 21.3.23.5.15.278	**FECHA DE APROBACIÓN:**	SISTEMA DE GESTIÓN DE LA CALIDAD CONCEJO MUNICIPAL DE SANTIAGO DE CALI	
	VERSIÓN: 06	**09-09-2020**		