EMPRESA PARA LA SEGURIDAD Y SOLUCIONES URBANAS - ESU

UNIDAD DE GESTION DOCUMENTAL

SISTEMA INTEGRADO DE CONSERVACION DOCUMENTAL

Versión 3
Enero de 2022
Jorge Iván Zapata – técnico administrativo grado 02

ESU - Carrera 48 # 20 - 114, Edificio Centro Empresarial Ciudad del Río, torre 3, piso 5
Teléfono: 444 34 48
info@esu.com.co - www.esu.com.co
Medellín - Antioquia

CONTENIDO

1. INTRODUCCION

La Ley 594 del 14 de Julio de 2000 (ley general de archivos) asignó la responsabilidad que tiene la administración pública y los funcionarios de archivo sobre la conservación de los documentos independientemente de su soporte.

Específicamente los artículos 46, 47 y 48 de la mencionada ley , así como los artículos 5 y 9 literal g del decreto 2609 de 2012, establecen la necesidad de implementar planes de conservación de documentos partiendo de las tablas de retención y valoración de documentos.

Para ello es necesario partir análisis técnicos sobre las condiciones de conservación física, electrónica, condiciones ambientales, operativas, análisis de riesgos, niveles de seguridad, perdurabilidad y formas de reproducción de la información.

Por otro lado, es necesario garantizar que materiales, espacios, procedimientos, equipos e instalaciones, cumplan las condiciones básicas para el correcto funcionamiento y conservación documental.

Se pretende dar cumplimiento a la obligación de implementar un sistema integrado de conservación de documentos para la Empresa para la Seguridad Urbana – ESU en cada una de las fases de los procesos del ciclo vital de los documentos.

Lo definimos como un conjunto de estrategias y procesos dirigidos a la conservación y preservación de la información acordes al sistema de gestión documental de la Empresa establecido por resolución 071 de 2006 con el objetivo de asegurar el adecuado cuidado de los documentos y garantizando la integridad física y funcional de toda la documentación, desde el momento de su emisión, durante su periodo de trámite su disposición final.

La preservación del material documental implica adelantar acciones de conservación preventiva que garanticen su preservación en el tiempo que se establece en las tablas de retención documental.

Finalmente pretendemos dar a conocer el alcance de las actividades y la metodología para desarrollarlas, todas ellas dirigidas a la ejecución del plan y a los recursos necesarios para llevarlas a cabo.

JORGE IVAN ZAPATA HENAO - TECNICO ADMINISTRATIVO

2. OBJETIVOS

- El Sistema de Conservación Documental del Concejo de la Empresa para la Seguridad Urbana – ESU, procura ejecutar y diseñar una matriz de acciones estratégicas contando con actividades de conservación y preservación, dentro del proceso de Gestión Documental, fundamentado en la noción de Archivo Total, cuyo propósito fundamental es el poder optimizar el mantenimiento de las condiciones operativas y ambientales, perdurabilidad, reproducción y seguridad de la información, garantizando la integridad tanto física como funcional de los documentos que produce o recibe la Empresa.

- Dar cumplimiento a lo establecido en los artículos 46, 47 y 48 de la ley 594 de 2000, decreto 2609 de 2012 artículos 5 y 9 literal g y al acuerdo 06 de 2014 expedido por el Archivo General de la Nación.

- Asignar responsabilidades para el desarrollo de las actividades encaminadas a la ejecución del plan de conservación documental a corto, mediano y largo plazo.

- Describir los diferentes componentes del sistema integrado de conservación incluyendo los componentes de archivo físico y electrónico.

- Contribuir de la mejor manera posible, desde el proceso de gestión documental, al desarrollo de las políticas de cero papel y eficiencia administrativa.

3. ALCANCE

El ámbito de aplicación es la Empresa para Seguridad Urbana ESU y su proveedor de servicios de outsourcing para custodia externa de archivo físico y medios magnéticos.
Involucra las actividades de todos los funcionarios relacionados el proceso de gestión documental.
El proceso de gestión dopcumental es transversal a todos los demás procesos, por lo tanto, involucra las actividades de producción y manejo de documentos en todas las áreas.

4. DEFINICION

Se define como el conjunto de actividades de preservación y conservación, acordes con el sistema de archivo central establecido en la entidad bajo el concepto de Archivo Total, para asegurar el adecuado mantenimiento de sus documentos, independientemente del tipo de soporte, garantizar la integridad física y funcional de toda la documentación, desde el momento de su emisión, durante su periodo de vigencia, hasta su depósito final o sea en cualquier etapa de su ciclo vital.

La preservación del material documental implica adelantar acciones de conservación preventiva y conservación donde se hará especial énfasis en la conservación preventiva. En este concepto se recogen los aspectos esenciales a partir de los cuales se deberán formular las políticas internas de preservación sea cual sea su naturaleza.

Las estrategias van dirigidas a garantizar la integridad física, la funcionalidad de los documentos la recuperación oportuna, el rearchivo y la disposición final de los mismos tal como lo establecen las TRD aprobadas para la entidad.

5. METODOLOGIA

5.1 IDENTIFICACION DE LA EMPRESA

La ESU es una empresa comercial e industrial del estado, de carácter territorial por pertenecer al municipio de Medellín, sus operaciones se realizan a nivel nacional y está registrada en la Cámara de Comercio de Medellín para Antioquia.

Tiene una estructura orgánica básica jerárquica conformada por: Junta Directiva, Gerencia, Secretaría General, Dirección Administrativa y Financiera, Dirección logística, Dirección Comercial, Dirección de Control Interno y Asesor de planeación.

La responsabilidad para la administración del proceso de gestión documental está en cabeza del funcionario Técnico Administrativo (según resolución 071 de 2006), responsabilidad refrendada por la Secretaría General, además, tiene a cargo el funcionamiento de la ventanilla única de radicación tal como se estipula en el acuerdo 060 del Archivo General de la Nación.

Administrativamente, L Unidad de Gestión Documental está adscrita a la Secretaría General.

Funciona bajo el esquema de Archivo Centralizado pues el control de la documentación es centralizado, la Entidad no cuenta con otras oficinas y en ninguna de las unidades administrativas se han establecido archivos de gestión.

El software de gestión documental tiene acceso remoto a través de internet y todos los funcionarios acceden a la información de manera limitada a sus funciones.

La Unidad de Gestión Documental cuenta con el mobiliario, equipos de cómputo y de digitalización de documentos adecuados a las necesidades de la Empresa.

5.2 UNIDAD DE GESTIÓN DOCUMENTAL

La Unidad de Gestión Documental, cuenta con manual de funciones claramente descritas y definidas para cada funcionario que allí labora.

Tiene su programa de gestión documental debidamente aprobado por el Comité de Archivo y tablas de retención documental aprobadas desde el año 2008.

En ésta Unidad se prestan los siguientes servicios:

- Consulta

Consulta manual de documentos

Se restringe este servicio con documentos físicos debido a que la mayoría de ellos, están digitalizados, esto hace parte de la primera acción de control relacionada con la preservación de documentos físicos.

Consulta electrónica de documentos

Todos los usuarios tienen acceso a la consulta de expedientes, los permisos se asignan de acuerdo con el perfil de las funciones de cada usuario.

Esta es la segunda medida de control de seguridad de la información.

Se dan autorizaciones especiales a algunos clientes, para que accedan remotamente a través de internet a algunos expedientes electrónicos.

- Mensajería

Para entrega de documentos y correspondencia a las entidades y personas con las cuales la ESU tiene algún tipo de relación.

El mensajero tiene la obligación de registrar todos los documentos entregados y devolver las copias radicadas en cada destino.

- Reproducción de documentos

Salvo casos especiales y por políticas de economía y de aplicación de la normativa 0 papel, no se imprimen documentos, a los usuarios se les envía la información utilizando medios magnéticos o correo electrónico.

- Asesoría

A todas las áreas en el manejo adecuado de sus documentos y los procesos documentales.

- Inducción

Como parte del programa de inducción, es obligatorio que todos los usuarios nuevos reciban la capacitación en el programa de gestión documental a través de inducción sobre el uso del software de gestión documental Mercurio.

Los usuarios antiguos reciben sesiones de reinducción con nuevos procedimientos, adiciones y mejoras en el programa.

5.3 USUARIOS

- Externos

Juzgados, Tribunales, Entes de Control, comunidad en general, proveedores, clientes, Dependencias del Municipio de Medellín, que buscan satisfacer la necesidad de información contenida en los documentos que produce la ESU.

- Usuarios Internos

Funcionarios vinculados, Contratistas, asesores.

5.4 INFRAESTRUCTURA FISICA

EDIFICACION

El edificio fue Construido entre loa años 2007 y 2008, está localizado en el siguiente contexto: por el norte zona verde cercada, de propiedad del municipio de Medellín; por el occidente con la carrera 48 avenida las Vegas, por el oriente con la carrera 47 y por el sur con la torre dos de la ciudadela empresarial Ciudad del Rio. Tiene 12 pisos y el archivo ocupa oficinas situadas en el quinto piso, sobre losa del cuarto piso nivel del parqueadero privado del edificio.

La edificación tiene buen excelente estado de conservación pues hace parte del desarrollo empresarial en la zona del conocido barrio Colombia de Medellín, zona comercial por excelencia, dotado de aire acondicionado modular y con planta de energía de emergencia.

Es un entorno de vocación comercial y urbanístico en pleno desarrollo ya que es la puerta de entrada a todo el sur del área metropolitana.

Está dotado de archivo rodante de cadena de tracción son 4 módulos dobles que consituyen 196 entrepaños o espacios con separadores metálicos en los cuales caben 50 a 60 carpetas en cada uno.

Tiene sistema anti incendio por irrigación en las oficinas contiguas, en la Unidad de Gestión Documental no existen, pero, tiene extintor de uso múltiple tipo ABC.

El área ocupada es de 34 m2.

5.5 CUSTODIA EXTERNA

El archivo histórico de la Empresa está bajo custodia externa de la Empresa Manejo Técnico de Información S.A. en bodega localizada en el corregimiento de la Tablaza, Municipio de la Estrella, Antioquia.

Es una bodega adecuada para conservar documentos físicos y medios magnéticos en ambientes de temperatura y humedad controlados, desinfectados y libres de plagas.

Los documentos se entregan en cajas de diseño especial, de resistencia adecuada, tamaño homogéneo y fabricadas en material neutro.

Temperatura ambiente 19 °C
Humedad relativa 61%

Este depósito cuenta con estantería pesada y tiene la capacidad suficiente para albergar por varios años la información que se le confíe. Presta además servicios de digitalización, guarda y custodia de títulos valores y conserva los medios magnéticos de la Empresa.

El acceso a la información solo se hace a personas registradas previamente en número máximo de dos personas.

5.6 CONDICIONES DE PREVENCION DE DESASTRES

- Existe Plan de Prevención de Desastres para la Edificación y plan de contingencia para la información.
- Existe detector de incendio.
- Existen centros cercanos de apoyo en caso de desastre.
- El edificio posee extintores y brigada de rescate
- En el archivo hay 1 extintor.
- Existe comité paritario de salud ocupacional.
- Existe brigada de evacuación.
- Existe Mapa de Riesgos para la Empresa
- Se hacen simulacros de evacuación.
- Existe señalización de puntos de encuentro.
- Existe vigilancia privada.
- Las condiciones de operación diaria son adecuadas e higiénicas lo cual no hace necesario el uso de elementos especiales de protección personal.
- No son necesarios extractores de polvo.
- El mantenimiento y limpieza tanto del archivo rodante se realiza cada 2 semanas.

5.7 ALMACENAMIENTO

El archivo de documentos se conforma por expedientes únicos y centralizados, es decir, todos los documentos generados durante la operación diaria, son enviados al archivo.

El control documental se lleva a cabo por medio del software de gestión documental mercurio.

Además de lo anterior, las condiciones de espacio de los puestos de trabajo de todas las áreas no permiten conformar archivos de gestión, lo que a su vez permite que no se generen transferencias de documentos.

El archivo conserva un total de 39.245 expedientes físicos y aproximadamente 2.4 millones de imágenes en base de datos.

5.8 DISTRIBUCION

La documentación se encuentra archivada según las tablas de retención documental debidamente aprobadas por el Consejo Departamental de Archivo.

Serie
Subserie
Asunto o tipo documental

Las fuentes de recuperación de documentos son el programa mercurio con sus módulos de inventario, consulta de expedientes y consulta de documentos recibidos internos y externos.

El archivo funciona como archivo central, regulando sus procedimientos de Producción, recuperación y disposición final de la documentación; no cuenta con cronograma de transferencias primarias (Archivo de Gestión a Central) por tratarse de un archivo de control centralizado, el paso de los documentos del archivo central al histórico se realiza de acuerdo con las Tablas de Retención Documental.

5.9 PRESERVACION DOCUMENTAL

No hay presencia de insectos voladores ni rastreros, roedores, hongos se hacen fumigaciones cada 6 meses

La ARL Colmena realiza controles de postura y actividades de pausas activas con los funcionarios y no hay evidencia de enfermedades profesionales en los funcionarios que administran la información física y electrónica.

Como primer tratamiento de conservación a los documentos se restringe la circulación de documentos físicos y les prohíbe a los funcionarios rayar, subrayar y hacer anotaciones sobre los documentos originales que circulan por las áreas.

La empresa cuenta con un manual de convivencia en el que se han establecido prácticas de higiene personal para todos los funcionarios incluyendo los que manejan información.

Dentro de las tareas del personal de aseo y cafetería se han implementado labores de limpieza de la oficina diarias, del mobiliario y archivadores cada dos semanas y de la documentación cada seis meses.

Se conoce y aplica normatividad sobre conservación expedida por el Archivo General de la Nación.

El Centro de Información Documental está dotado de los materiales suficientes que se utilizan para la producción y almacenamiento de documentos: carpetas, ganchos de legajar, adhesivos de identificación, cajas, estanterías.

Aunque no se cuenta con equipos para el control de humedad sí es posible controlar la temperatura, la cual a su vez, contribuye a controlar el factor de humedad.

Como política de conservación de documentos originales, no se realiza encuadernación de documentos.

La Unidad de Gestión Documental cuenta con su programa de gestión documental debidamente aprobado por el Comité de Archivo, en el cual también se describen las actividades de conservación y disposición de los documentos.

5.10 PRESUPUESTO

El archivo no cuenta con rubro específico para su funcionamiento, sus necesidades se satisfacen con relación al presupuesto integral de la ESU, de acuerdo con los requerimientos de operación diaria.

Los proyectos y actividades adicionales se discuten y aprueban dentro de las reuniones del del Sistema Integrado de Gestión y son puestos a consideración de la gerencia para el respectivo manejo financiero.

6. POLITICAS INTERNAS DE PRESERVACION DE DOCUMENTOS

6.1 DESDE LA ORGANIZACIÓN DOCUMENTAL

Se han establecido estrategias en el plan de acción dirigidas a garantizar la integridad física como funcional de los documentos físicos y electrónicos.

Los documentos electrónicos tienen los niveles de seguridad necesarios para garantizar los valores propios de cada uno de ellos: originalidad, integridad y funcionalidad.

6.2 DESDE LOS ARCHIVOS DE GESTION

Como la Empresa para la Seguridad y Soluciones Urbanas – ESU tiene conformado un archivo centralizado y su sistema de gestión documental también lo es, y que la inmensa mayoría de los documentos se transan de manera electrónica, y que el diseño de las oficinas y puestos de trabajo no permiten la creación de archivos satélites, se ha dispuesto que no se generarán archivos de gestión y que este será el que cada usuario conserva en su carpeta electrónica.

La responsabilidad especial y obligaciones del servidor público al desvincularse de las funciones titulares, deberá entregar los documentos y archivos a su cargo debidamente inventariados, conforme a las normas y procedimientos, sin que ello implique exoneración de las responsabilidades a que haya lugar en caso de irregularidades según lo estipula el numeral 5 del artículo 34 de la Ley 734 de 2002.

Se aplica la directiva presidencial 04 para la implementación de las oficinas 0 papel por lo tanto, se emplea de manera adecuada la técnica reprográfica restringiendo el uso de fotocopias, utilizando la reproducción electrónica y magnética.

Reciclaje de materiales de archivo en buenas condiciones: cajas, carpetas y ganchos.

Revisar con frecuencia las instalaciones eléctricas e hidráulicas, los equipos de iluminación, sensores de humo, alarmas de incendio.

Mantenimientos periódicos a los equipos de captura de imágenes, computadores, servidores y bases de datos.

6.3 DESDE LA PRODUCCION DE DOCUMENTOS

Cuando la documentación que se va a producir se enmarca dentro de la documentación con valor primario y/o secundario, con condiciones de carácter permanente, debe ser elaborada y radicada en el sistema de gestión documental, siguiendo parámetros que cumplan condiciones de conservación.

Los papeles utilizados como soporte y las tintas para consignar la información, deben ser estables químicamente bajo condiciones normales de humedad relativa y temperatura. En lo posible utilizar papel libre de cloro o papel alcalino que por su naturaleza básica y su estabilidad química garantizan la permanencia del soporte.
Del mismo modo, es necesario imprimir los documentos en impresora láser. Este sistema utiliza tintas estables, y su sistema de impresión al calor, brinda condiciones de permanencia para la documentación de archivo.

Es necesario garantizar impresión firme en los documentos que se van a digitalizar, para las firmas se recomienda el uso de tintas esferográficas, las cuales presentan estabilidad química y son absorbidas adecuadamente por el papel sin producir manchas.

Tener en cuenta los instructivos para la elaboración de: Cartas, Memorandos, circulares y Actas para la producción de estos documentos.

De igual forma, tener en cuenta los formatos que han sido aprobados por el Comité de Archivo de la Empresa y que hacen parte del sistema de calidad

6.4 DESDE LA UNIDAD DE GESTIÓN DOCUMENTAL

En coordinación con el funcionario responsable de Gestión Documental y el Comité Integrado de Gestión se planean, programan, ejecutan y coordinan las actividades inherentes a la Gestión Documental de la Empresa, para la administración de los documentos en sus diferentes fases gestión, central e Histórica.

7. RECOMENDACIONES SOBRE FACTORES DE DETERIORO

Programar el saneamiento semestral de las áreas de trabajo, con la participación del Comité Paritario de Seguridad y Salud en el trabajo.

Evitar el uso de cintas adhesivas, gomas y líquidos pegantes en el papel de archivo.

La labor de envío y recepción de los documentos almacenados en custodia externa, debe realizarse con clima sin lluvia, en caso contrario debe proveerse la protección impermeable adecuada para protección del cartón.

Al momento de recibir documentos que han sido prestados se debe verificar el estado en que son devueltos: orden de los de documentos sin alterar, documentos completos y en buen estado.

Evitar el uso de lápices y bolígrafos para señalar documentos.

Hacer uso mínimo del servicio de reproducción de documentos ofrecido por la entidad.

No utilizar separadores, ni permitir el uso de bolsos o carteras.

Disponer de elementos de papelería para humedecer los dedos, no usar saliva en ningún caso.

8. PROGRAMA DE LIMPIEZA DEL ARCHIVO Y LOS DOCUMENTOS

Consiste en planear, ejecutar, verificar y tomar medidas correctivas si es el caso, tendientes a remover la suciedad existente en los elementos y/o documentos de uso permanente que quieren pulcritud para su manejo, contribuyendo a conservar la salud y mejoramiento del clima laboral de quienes los utiliza.

8.1 OBJETIVOS DEL PROGRAMA DE LIMPIEZA

- Contribuir a la conservación de documentos.
- Generar un ambiente laboral adecuado en las oficinas.
- Estimular hábitos de limpieza.
- Mejorar la presentación de los puestos de trabajo.
- Aplicar postulados del manual de convivencia laboral.

8.2 SUGERENCIAS PARA LIMPIEZA EFICIENTE

En un ambiente contaminado se deben seguir las normas básicas de higiene preventiva:

- Retirar todos los objetos que se tenga en las manos como por ejemplo anillos, relojes, pulseras, entre otros.

- Humedecer las manos y aplicar jabón antiséptico, frotando vigorosamente dedo por dedo, haciendo énfasis en los espacios interdigitales. Frotar palmas y dorso de las manos, cinco cm por encima de la muñeca. Enjuague las manos con abundante agua para que el barrido sea efectivo. Finalice secando con toallas desechables.

- Lavar las mucosas nasales con suero fisiológico.

- Se debe realizar descansos de 15 minutos, después de dos horas de trabajo.

8.3 LIMPIEZA

La limpieza y remoción de polvo y suciedad es función del personal de aseo y cafetería adscrito a la Subgerencia Administrativa, sin embargo, es responsabilidad de todo el personal de la Unidad de gestión Documental velar porque los puestos de trabajo se mantengan en condiciones óptimas.

El área de Gestión Humana está en la obligación de dictar charlas sobre el manejo de productos y procedimientos adecuados para una correcta labor de limpieza y aseo como parte del proceso junto con el proveedor del servicio externo.

Sensibilización a las personas encargadas de la función de limpieza y aseo sobre la importancia del seguimiento a un programa de limpieza y aseo.

Los elementos que se utilicen en la rutina de limpieza deben ser exclusivos de estas áreas o depósitos, pues se pueden propagar agentes infecciosos de las demás dependencias o viceversa.

Dos veces en el mes, se hará una limpieza profunda de estanterías, repisas, archivadores.

La limpieza de pisos y tapetes se realizará con aspiradora, de esta forma se evitará levantar el polvo, o en su defecto, con un trapeador impregnado ligeramente con un limpiador para pisos y pasarlo en zig-zag, empezando de la zona más sucia a la que presenta menor suciedad, no utilizar detergentes, ni blanqueadores.

Para las paredes, mobiliario y demás elementos, lo ideal es el uso de aspiradora, sin embargo en caso de no contar con este implemento, se utilizará una tela o trapo de algodón siempre seco, pasando por el área menos sucia a la más sucia.

Limpiar las mesas de trabajo con limpiadores antisépticos.

La limpieza de aparatos tecnológicos como computadores y escáner son responsabilidad del área de tecnología y son ellos los que determinarán la periodicidad de los mantenimientos.

Mantener los elementos de protección en óptimas condiciones de aseo, en un lugar seguro y de fácil acceso.

Los traperos y/o trapos usados deben primero ser lavados y luego desinfectados.

9. CONDICIONES AMBIENTALES

Las condiciones ambientales especificadas para la conservación de documentos en la Empresa para la Seguridad Urbana es la siguiente:

Temperatura de 17 a 21 grados centígrados 3 grados.

Humedad relativa entre 45% y 61% con fluctuación diaria del 5%.

Para medios magnéticos y servidores:

Temperatura 14 a 10 grados centígrados

Humedad relativa de 40% a 50%

Ventilación de caudal continuo variable localmente según condiciones climáticas externas.

Las cajas que se utilizan para almacenar carpetas, legajos o libros, protegen la documentación del polvo, la contaminación, los cambios bruscos de humedad relativa y temperatura, y contribuyen a su adecuada manipulación y organización.

Material para las cajas

Cajas producidas con cartón kraft de (220 gr x metro cuadrado) corrugado de pared sencilla.

Resistencia: El cartón corrugado debe tener una resistencia mínima a la compresión vertical de 930 Kgf/m2 y una resistencia mínima al aplastamiento horizontal de 2 Kgf/cm2.
Recubrimiento interno.

La composición del cartón debe tener ph neutro = 7 para evitar la migración de ácido a los documentos.

En ningún caso se deben usar cartones que tengan un recubrimiento cuyo único componente sea parafina.

Acabado: El cartón corrugado debe tener un acabado liso, suave, libre de partículas abrasivas u otras imperfecciones.

Solo se deben utilizar cajas de referencia comercial X300 de tamaño estándar por condicionamiento acordado con el proveedor del servicio de custodia externa.

Las cajas han ser funcionales y para ello se deben seleccionar diseños acordes con el formato de los documentos.

10. ESPECIFICACIONES CARPETAS DE ARCHIVO

Portada y contraportada en cartón kraft de ph neutro de 237 gr x metro cuadrado laminadas con película poliesterica de alta densidad adherida al calor a los demás elementos, de tamaño 22 x 35 cm

Deben estar troqueladas para el doblaje de las pestañas del gancho legajador y con perforaciones para gancho de legajar 8X2.

La cartulina debe tener un acabado liso, suave, libre de partículas abrasivas u otras imperfecciones.

En un lugar visible y de acuerdo con el diseño adoptado, se debe consignar la identificación de su contenido.

En la Unidad de Gestión Documental no se reciben documentos en folder A-Z por costo y poca funcionalidad para el almacenamiento de la documentación.

Las especificaciones técnicas de los extintores y el número de unidades deberá estar acorde con las dimensiones del depósito y la capacidad de almacenamiento. Implementar sistemas de alarma contra incendio y robo.

11. DISPOSICION FINAL DE DOCUMENTOS

Disponer de los documento como una decisión, es el resultado del proceso de implementación de las TRD y la valoración de todos los tipos documental que se manejan en la Organización, aplicada en cual fase del ciclo vital de los documentos.

Todas las depuraciones de documentos de la Empresa para la Seguridad Urbana, será llevada a cabo por intermedio de la Unidad de Gestión Documental, previo análisis y aprobación de Comité del Sistema Integrado de Gestión, decisión que deberá ser sustentada mediante acta escrita de la reunión aprobatoria.

Ninguna área de la Empresa está autorizada para eliminar documentos sin antes cumplir con el proceso de aprobación por parte del Comité del Sistema Integrado de Gestión.

Es el resultado de la aplicación de la TRD y TVD que ya han cumplido su ciclo vital, han perdido sus valores primarios o cuyo objetivo para el que fueron creados ya está cumplido, sin perjuicio de que la información contenida en ellos ya esté en otro formato o base de datos.

Toda la información digitalizada será conservada en diferentes bases de datos según su antigüedad.

Los líderes de tecnológica y de la Unidad de Gestión documental serán los responsables de elaborar los mapas migratorios cuando ocurran cambios tecnológicos, de software o hardware.

12. CRITERIOS PARA ELIMINAR DOCUMENTOS

Se debe asegurar la conservación de las cintas respaldo de las transacciones realizadas en el software de gestión documental.

La decisión de eliminar documentos, es responsabilidad del Comité del Sistema Integrado de gestión.

El principio que debe observarse es aquel según el cual los documentos que deben eliminarse, corresponden a lo señalado en las tablas de retención documental y ninguna serie documental puede ser destruida sin estar previamente registrada en la correspondiente tabla de retención.

Las eliminaciones deben formar parte del proceso de análisis preventivo de conservación documental puesto que el sistema de gestión documental es centralizado y no existen archivos de gestión.

En todos los casos siempre debe levantarse un acta acompañada de un inventario de todos los documentos eliminados.

Todas las eliminaciones de documentos se deben hacer por rasgado y/o picado mecánico.
Los medios magnéticos serán borrados antes de proceder a su destrucción.

13. CONSERVACIÓN TOTAL

Se aplica para documentos que tienen valor histórico para la Empresa, es un valor permanente en el tiempo y para aquellos que por disposición legal sea necesario conservar.

Todos los documentos de conservación total están relacionados en las tablas de retención documental.

Se tiene en cuenta las circunstancias propias de su producción:

Medio de producción del documento.
Ente / área generador.
Motivo generador del documento.
Serie documental.
Requisito legal para su producción y amparo.
Situación social en la que se produjo.

14. SELECCIÓN

No se harán selecciones de documentos que vayan a ser eliminados como muestras para conservación representativa, pues al conservar documentos digitalizados, también se conserva la representación de los documentos, su función y el papel cumplido durante el proceso de gestión.

Sin embargo para documentos que pertenezcan a series documentales que ya perdieron su vigencia y cuyo volumen es significativo o su contenido está descrito en otras series, o que se originaron por operación de procesos electrónicos, se permitirá hacer selección de aquellos que ameriten ser conservados.

15. MANUAL DE SEGURIDAD DE LA INFORMACIÓN

RESOLUCIÓN NÚMERO 098 DE 2015
(Enero 30 de 2015)

"Por medio de la cual se expide el Manual de Políticas y Estándares de Seguridad de la Información de la ESU"

El Gerente de la Empresa Para la Seguridad Urbana – ESU

En uso de las facultades legales conferidas por el Decreto Municipal 178 de 2002 y la Ley 489 de 1998, y

Considerando:

La Empresa para la Seguridad Urbana -ESU-, consciente de la importancia que representan los activos de información y teniendo en cuenta su valor en la operación y en la gestión de la Entidad como medio para alcanzar los objetivos estratégicos propuestos, y reconociendo que aunque la aparición de nuevas tecnologías representa grandes avances en el manejo de la información, también trae consigo amenazas, que de no ser detectadas oportunamente, pueden materializarse

en riesgos que deberán ser mitigados, decide implementar un modelo de Gestión de Seguridad de la Información, de acuerdo con los lineamientos definidos por el Departamento Administrativo de la Función Pública, en lo concerniente al Modelo Integrado de Planeación y Gestión, y al Programa de Gobierno en Línea del Ministerio de Tecnologías de la Información y las Comunicaciones.

La Empresa para la Seguridad Urbana para el cumplimiento de su misión, visión, objetivos estratégicos, y apegada a sus valores corporativos, establece el Manual de Políticas y Estándares de Seguridad de la Información, con los siguientes objetivos:

Objetivo General:

Desarrollar estrategias que orienten el uso adecuado de las herramientas y recursos tecnológicos, para minimizar los riesgos a los cuales se expone la información y sacar el mayor provecho de las ventajas que ofrecen en beneficio de la entidad.

Objetivos Específicos:

- Minimizar el riesgo asociado con la seguridad de la información, en los procesos más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los lineamientos establecidos por el Departamento Administrativo de la Función Pública, en lo concerniente al Modelo Integrado de Planeación y Gestión, y al Programa de Gobierno en Línea del Ministerio de Tecnologías de la Información y las Comunicaciones
- Apoyar la innovación tecnológica.
- Implementar el Plan de Copias de seguridad de la información.
- 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 de la entidad, practicantes y contratistas.
- Garantizar la continuidad de los procesos de negocio frente a incidentes de la plataforma tecnológica

Este manual de políticas y estándares será de obligatorio cumplimiento por parte de quienes tengan acceso a los recursos o servicios informáticos de la ESU y se aplicará indistintamente si la entidad posee o no la propiedad de dichos recursos o servicios.

Será revisado por el comité de Gobierno en Línea anualmente con un seguimiento trimestral o cuando se identifiquen cambios significativos en el negocio que influyan en su estructura, sus objetivos o alguna condición que afecten las políticas, para asegurar que sigue siendo adecuado y ajustado a los requerimientos identificados.

POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

1. La Empresa para la Seguridad Urbana – ESU ha establecido las siguientes Políticas Generales de Seguridad de la Información, las cuales representan la visión de la Entidad en cuanto a la protección de sus activos de Información:

2. Definir un Comité de Seguridad de la Información, que será el responsable del mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información, que para la ESU es el mismo comité de Gobierno en Línea.

3. Identificar y clasificar los activos de información de la ESU, para establecer los mecanismos de protección necesarios correspondientes.

4. Definir e implantar controles para proteger la información contra violaciones de autenticidad, accesos no autorizados y pérdida de integridad, que respondan a la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la Entidad.

5. Proteger la información a la que se acceda y procese, para evitar su pérdida, alteración, destrucción o uso indebido.

6. Realizar seguimiento y control periódico sobre el modelo de gestión de Seguridad de la Información de la ESU, para verificar su eficiencia y aplicabilidad.

7. Permitir únicamente el uso de software que haya sido adquirido legalmente por la Institución y previamente autorizado por el proceso de Tecnológica de la Información.

8. Reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los recursos que un funcionario y/o contratista identifique, a través del procedimiento establecido por la mesa de ayuda.

9. Registrar y monitorear las violaciones a las Políticas y Controles de Seguridad de la Información, y a su vez reportarlas a la Secretaría General para que dé inicio a las investigaciones pertinentes de conformidad con su competencia disciplinaria interna y a lo establecido en el Código Disciplinario Único y demás normas relacionadas.

10. Incluir este manual como parte integral del procedimiento de Inducción del Área de Gestión Humana de la Empresa para la Seguridad Urbana.

Además de las políticas generales dispuestas a cumplir en la Empresa para la Seguridad Urbana, se adoptarán las estrategias para la seguridad de la información definidas en la NTC ISO 27001:2013, y las que la Entidad ha dispuesto a partir del análisis de los riesgos de la seguridad de la Información.

ESTRATEGIA: SEGURIDAD DE LA INFORMACIÓN EN LA CONTRATACIÓN

Políticas:

- Identificar los riesgos asociados al acceso, procesamiento, comunicación o gestión de la información y/o la infraestructura para su procesamiento, por parte de personas o entidades externas, terceros y/o contratistas, con el fin de establecer los mecanismos de control necesarios para que la seguridad se mantenga.

- Definir una cláusula de confidencialidad de la información como parte integral en los contratos de trabajo y en los contratos con personas o entidades externas, terceros y/o contratistas, cuando deban tener acceso a la información y/o recursos de la Entidad; además, de no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos para la clasificación de la información, teniendo en cuenta que cualquier violación a lo establecido en dicha cláusula será considerado como un "incidente de seguridad".

ESTRATEGIA: USO EFICIENTE DE LOS ACTIVOS DE INFORMACIÓN

Políticas:

- Los activos de información disponibles para los servidores, contratistas y/o terceros, para su uso, operación y/o custodia, de acuerdo a las funciones específicas y necesidades del trabajo a realizar son propiedad exclusiva de la ESU.

- Restringir el acceso a los documentos físicos y digitales según las normas aplicables internas y/o externas, y a los permisos determinados de acuerdo con las funciones del perfil de cargos.

- Toda la información de los procesos de la ESU, así como los activos donde ésta se almacena y se procesa están:

  - Inventariados.
  - Asignados a un responsable.
  - Protegidos y clasificados. De acuerdo con la clasificación se deben establecer los niveles de protección orientados a determinar a quién se le permite el manejo de la información, el nivel de acceso a la misma y los procedimientos para su manipulación.

- Revisar la identificación y la clasificación de los activos de información anualmente y/o cuando se presenten cambios que puedan afectar las mismas.

- Todos los funcionarios y/o contratistas de la Entidad son responsables de la gestión y protección de los activos de información que se encuentren a su cargo o a los que tengan acceso; de tal forma que se mantengan los niveles de seguridad a lo largo del ciclo de vida de la información.

- El Proceso de Gestión de Tecnología de la Información es el único autorizado para la instalación de cualquier tipo de software o hardware en la Entidad, más no de la manipulación de la información que se genere dentro de los procesos.

- Asignar a cada funcionario, personal en misión, practicantes y/o contratista que ingrese a la Entidad los activos de información previa solicitud del área del proceso de Gestión del Talento Humano según el procedimiento establecido; con una anticipación de cinco (5) días hábiles, donde se especifique el nombre completo y cédula del funcionario, el tipo de equipo, aplicativos y permisos a asignar, la fecha de ingreso y su ubicación. El proceso de Gestión del Talento Humano deberá notificar con una anticipación de cinco (5) días hábiles el retiro del funcionario y/o contratista, para realizar las respectivas copias de seguridad y la desactivación del usuario.

- Entregar mediante acta a cada funcionario y/o contratista de la Entidad los activos de información asignados, donde reconozca y acepte toda responsabilidad sobre el estado de los mismos al momento de su devolución y donde individualmente se compromete a salvaguardar y usar correctamente dichos activos.

- Definir el software y aplicaciones que se encuentran permitidas para ser instaladas en las estaciones de trabajo de la Entidad.

- Realizar seguimiento y control anualmente al licenciamiento del software y aplicaciones de la Entidad.

- El proceso de Gestión de Tecnología de la Información, es el único autorizado para realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, conexiones de red, usuarios locales de la máquina, entre otros.

- Notificar al proceso de Gestión de Tecnología de la Información, a través del procedimiento establecido, cuando sea vaya a retirar un activo de tecnología de la entidad, especificando la fecha y hora de retiro del equipo, el tiempo que estará por fuera de las instalaciones y el lugar donde se encontrará el mismo. Esta información podrá ser corroborada con el jefe inmediato o el director del área correspondiente.

- Asegurar todos los equipos de la entidad contra todo riesgo, daño, pérdida o robo. Ante cualquier incidente de dicha naturaleza el funcionario informará inmediatamente al proceso de Gestión de Tecnología de la Información, a través del procedimiento establecido, especificando el tipo, modo, tiempo y lugar del incidente para iniciar lo establecido en la política de activos de la entidad.

- Proteger adecuadamente todos los equipos que hacen parte de la infraestructura tecnológica de la ESU para prevenir la pérdida, el daño, el robo o los accesos no autorizados; y ubicarlos alejados de sitios que puedan tener amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética, vandalismo, entre otros.

- Los equipos de Cómputo Fijos que se asignen a cada uno de los funcionarios y/o contratistas de la entidad, sólo podrán ser reubicados por el proceso de Gestión de Tecnología de la Información o Gestión de Infraestructura.

- Evitar fumar, beber o consumir algún tipo de alimento cerca de los equipos que componen la infraestructura tecnológica de la ESU.

ESTRATEGIA: CONTROL PERMANENTE SEGÚN LAS FUNCIONES DE LOS PERFILES

Políticas:

- Definir los roles y responsabilidades, frente al nivel de acceso y los privilegios de los funcionarios que tengan acceso a la infraestructura tecnológica y a los sistemas de información de la Empresa, con el fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información de la entidad.

- Implementar reglas de control de acceso para todos los sistemas de disponibilidad crítica o media de la Entidad, de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

- Establecer controles duales sobre el nivel de súper usuario de los sistemas de información, de tal forma que exista supervisión a las actividades realizadas por el administrador del sistema.

ESTRATEGIA: SEGURIDAD DE LA INFORMACIÓN EN LAS REDES CORPORATIVAS

Políticas:

- Separar la red en segmentos físicos y lógicos para independizar la red de usuarios de conexiones con terceros y del servicio de acceso a Internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad si así se requiere. El proceso de Gestión de Tecnología de la Información es el encargado de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

- Establecer mecanismos de identificación automática de los equipos en la red, como medio de autenticación de conexiones, desde segmentos de red específicos hacia las plataformas donde operan los sistemas de información de la Entidad.

- Garantizar que los puertos físicos y lógicos de diagnóstico y configuración de los equipos que soportan los sistemas de información estén siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.

- Conectar a la red inalámbrica corporativa de la Entidad únicamente los equipos de cómputo asignados a los funcionarios y/o contratistas desde el proceso de Gestión de Tecnología de la Información, por consiguiente está prohibido conectar cualquier dispositivo móvil.

- Solicitar al proceso de Gestión de Tecnología de la Información, el establecimiento de una conexión a la infraestructura tecnológica de la ESU para los terceros que así lo requieran; esta solo se realizará a través de la red Inalámbrica de Invitados y será válida por 4 horas máximo.

- Prohibir a los funcionarios y/o terceros la conexión a la red LAN o WLAN de cualquier equipo por fuera del dominio esu.com.co.

ESTRATEGIA: CONTROL EFICIENTE EN EL ACCESO FÍSICO Y LÓGICO

Políticas:

- Asignar el acceso a los recursos de información de la Entidad de acuerdo a la identificación previa de requerimientos de seguridad y del negocio que se establezcan en el manual de perfil de cargos de la Entidad, así como las normas legales o leyes de protección de acceso a la información aplicables.

- Establecer medidas de control de acceso físico en el perímetro que puedan ser auditadas, así como procedimientos de seguridad que permitan proteger la información, el software y el hardware de daños intencionales o accidentales para todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones.

- Contar con mecanismos que permitan monitorear y garantizar que se cumplen los requerimientos ambientales (temperatura, humedad, etc.), especificados por los fabricantes de los equipos y que pueden responder de manera adecuada ante incidentes como incendios e inundaciones en los centros de cómputo, cableado y cuartos técnicos de las oficinas.

- Utilizar siempre cifrado de datos para las conexiones remotas a la infraestructura tecnológica de la entidad, las cuales serán otorgadas por el proceso de Gestión de Tecnología de la Información, de acuerdo con las necesidades de cada usuario y previa autorización del Director del área correspondiente; será responsabilidad de cada usuario velar por la seguridad, confidencialidad e integridad de la información a la que tiene acceso de forma remota.

ESTRATEGIA: USO EFICIENTE DEL CORREO ELECTRÓNICO Y DE LAS HERRAMIENTAS DE COLABORACIÓN

Políticas:

- Usar la cuenta de correo electrónico asignada únicamente para el desempeño de las funciones dentro de la entidad.

- Los mensajes y la información contenida en las cuentas de correo (entendiéndose por esto el buzón y demás aplicativos de colaboración) son propiedad de la Entidad, y cada usuario como responsable de su buzón, debe mantener solamente información relacionada con el desarrollo de sus funciones.

- El tamaño de los buzones de correo electrónico es de 30 Gb; si un usuario requiere espacio adicional, deberá solicitarlo al proceso de Gestión de Tecnología de la Información, quien tendrá potestad para determinar o no, la viabilidad de la solicitud.

- Solo se podrán enviar y/o recibir correos electrónicos que tengan un peso máximo de 25 Mb.

- Compartir información por el aplicativo Google Drive, únicamente con usuarios internos de la Entidad; en caso de requerir compartir archivos con usuarios externos deberá ser autorizado por el Proceso de Gestión de Tecnología de la Información.

- Las conversaciones por el Chat corporativo Gtalk o Hangouts con terceros externos a la entidad sólo están permitidas para el desarrollo de las funciones propias del cargo; teniendo en cuenta que es una herramienta para facilitar la comunicación es obligatorio estar siempre conectado y en modo visible mientras se esté en el ejercicio de sus funciones.

- Enviar la información corporativa exclusivamente desde la cuenta de correo que la ESU proporciona.

- Para enviar mensajes publicitarios corporativos el proceso de Gestión de Tecnología de la Información es el autorizado para aprobar la solicitud presentada por el proceso de Gestión de la Comunicación; con el fin de evitar posibles bloqueos o inclusiones en listas negras.

- Incluir en los mensajes publicitarios corporativos enviados a terceros por medio del correo electrónico, un mensaje que le indique al destinatario como ser eliminado de la lista de distribución.

- Todos los Grupos de Distribución serán creados y configurados por el Proceso de Gestión de Tecnología de la Información, previa solicitud del proceso de Gestión de la Comunicación.

- Toda información de la ESU generada con los diferentes programas computacionales (Ej. Office, Project, Access, Wordpad, etc.), que requiera ser enviada fuera de la Entidad, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

- Todas las firmas predeterminadas y el pie de página de los correos electrónicos, serán configurados por el Proceso de Gestión de Tecnología de la Información, previa solicitud del proceso de Gestión de la Comunicación.

- No es permitido:

    - Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y/o la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Entidad; de igual forma mensajes malintencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.

    - Utilizar la dirección de correo electrónico de la ESU como punto de contacto en comunidades interactivas de contacto social, tales como facebook y/o Twitter o cualquier otro sitio que no tenga que ver con las actividades laborales.

    - Enviar archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

    - Enviar y/o recibir archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por el Proceso de Gestión de Tecnología de la Información.

    - Entregar la lista de correo electrónico de los funcionarios de la Entidad, a usuarios externos que la utilicen para fines comerciales o políticos.

    - Abrir correos electrónicos de remitentes desconocidos o que sean sospechosos de tener contenido malintencionado como virus o malware.

- Intercambiar información no autorizada de propiedad de la ESU, de sus clientes y/o de sus funcionarios, con terceros.

ESTRATEGIA: ACCESO A INTERNET

Políticas:

- Controlar, verificar y monitorear la Información, el uso y la navegación en internet de todos los usuarios tanto funcionarios como invitados o terceros que se conecten a la red de la entidad para navegar en internet de manera permanente, con el fin de garantizar el uso eficiente del canal corporativo y mantener la seguridad de la información.

- Realizar monitoreo permanente de los tiempos de navegación y páginas visitadas por parte de los funcionarios y/o terceros. Así mismo, inspeccionar, registrar y evaluar las actividades realizadas durante la navegación, de acuerdo a la legislación nacional vigente.

- Dar un uso adecuado a este recurso y en ningún momento usarlo para realizar prácticas ilícitas o malintencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

- No está permitido:

    - Acceder a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética, las leyes vigentes o políticas establecidas en el presente manual.

    - Acceder y usar servicios interactivos o mensajería instantánea como Facebook, Instagram, MSN Messenger, Yahoo, Skype, Net2phone y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio de la ESU.

    - Descarga, usar, intercambiar y/o instalar juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, archivos ejecutables, información y/o productos que de alguna forma atenten contra la propiedad intelectual, a su vez, herramientas que comprometan la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica de la Entidad.

    - Descargar, instalar, compartir o usar información audiovisual (videos e imágenes) utilizando sitios públicos en Internet. De requerirse esta situación, el proceso de Gestión de Tecnología de la Información, o a quienes ellos deleguen de forma explícita para esta función, deben autorizarlo asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

    - Asumir en nombre de la ESU, posiciones personales en encuestas de opinión, foros u otros medios similares por ningún funcionario y/o tercero, al igual que los empleados o subcontratistas de estos.

ESTRATEGIA: PROTECCIÓN PERMANENTE CONTRA SOFTWARE MALICIOSO

Políticas:

- Proteger todos los recursos informáticos mediante herramientas y software de seguridad como antivirus, antispam, antispyware y otras aplicaciones que brinden protección contra código malicioso y prevenir el ingreso del mismo a la red de la Entidad.

- Contar con controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código móvil y malicioso. Será responsabilidad del proceso de Gestión de Tecnología de la Información autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados bajo ninguna circunstancia, así como de su actualización permanente.

- Asegurar que el análisis de seguridad y desinfección por medio del antivirus sea ejecutado a todos los dispositivos de almacenamiento una vez estos sean conectados al equipo.

- No está permitido:

    - Desinstalar y/o desactivar el software y/o herramientas de seguridad avaladas previamente por la ESU.

    - Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.

    - Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.

    - Usar código móvil que no haya sido debidamente autorizado por el proceso de Gestión de Tecnología de la Información.

ESTRATEGIA: GESTIÓN EFECTIVA DE LAS COPIAS DE SEGURIDAD

Políticas:

- Asegurar que la información con cierto nivel de clasificación, contenida en la plataforma tecnológica de la Entidad, como servidores, dispositivos de red para almacenamiento, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad.

- Mantener un plan de restauración de copias de seguridad y revisarlo periódicamente, con el fin de asegurar que las copias sean confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

- Establecer procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia e identificación de los respaldos.

- Definir conjuntamente con la Alta Gerencia y de acuerdo a lo determinado por la ley, los períodos de retención de las copias de seguridad y disponer de los recursos necesarios para identificar los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos, permitiendo un rápido y eficiente acceso a los medios que contienen la información resguardada.

- Almacenar en un sitio externo los medios magnéticos que contienen las copias de seguridad de la Entidad; Dicho sitio debe tener los controles de seguridad adecuados, cumplir con máximas medidas de protección y seguridad física apropiada.

- Respaldar diariamente la información que se encuentre en las carpetas Mis Documentos, Mis Imágenes, o en el Escritorio de los usuarios que tengan asignados recursos virtualizados. Toda información almacenada en una ubicación diferente no será respaldada.

- Respaldar diariamente la información de la carpeta "RESPALDO" creada por el Proceso de Gestión de Tecnología de la Información, en el Escritorio de los usuarios que tienen equipos portátiles o PCs. Es responsabilidad de cada usuario almacenar la información crítica y de vital importancia en dicha carpeta, teniendo en cuenta que la información por fuera de esta carpeta no será respaldada.

- Respaldar mensualmente la información de los dispositivos móviles corporativos.

- Eliminar la información alojada en los servidores que no tenga relación con la ejecución de los procesos de la Entidad.

- Excluir del proceso de respaldo los archivos con extensiones .exe, .mp3.

ESTRATEGIA: SEGURIDAD DE LA INFORMACIÓN PARA LOS MEDIOS EXTRAÍBLES.

Políticas:

- Autorizar el uso de medios de almacenamiento removibles (CDs, DVDs, USBs, memorias flash, discos duros externos, Ipods, celulares, cintas) sólo a aquellos funcionarios cuyo perfil del cargo y funciones así lo requieran, previa comunicación escrita del Director del Área correspondiente al proceso de Gestión de Tecnología de la Información.

- Implementar los controles necesarios para asegurar que en los sistemas de información de la Entidad sólo los funcionarios autorizados pueden hacer uso de los medios de almacenamiento extraíbles.

- Asegurar física y lógicamente los dispositivos extraíbles con el fin de no poner en riesgo la información de la ESU contenida en los mismos.

ESTRATEGIA: USO EFECTIVO DE LAS CONTRASEÑAS DE USUARIO ASIGNADAS.

Políticas:

- Todo funcionario o tercero que requiera acceso a los sistemas de información de la ESU debe contar con un usuario (ID) y contraseña (password) asignado por el proceso de Gestión de Tecnología de la Información. El funcionario será responsable por el buen uso de las credenciales de acceso asignadas y el cumplimiento de las políticas descritas en este manual.

- Las contraseñas de acceso a los diferentes sistemas de información, no deben compartirse o revelarse a otros personas y/o usuarios; el hacerlo expone al usuario a las consecuencias disciplinarias y/o judiciales, por las acciones que los otros hagan con la misma.

- Cambiar la contraseña cada mes cumpliendo con las condiciones mínimas de longitud y complejidad establecidas por el proceso de Gestión de Tecnología de la Información.

ESTRATEGIA: SEGURIDAD PERMANENTE DEL USUARIO

Políticas:

- Mantener la información restringida o confidencial bajo llave o bloqueada con contraseña, en todo momento, en especial cuando el puesto de trabajo se encuentra desatendido, al igual que en las horas no laborales, con el fin de evitar pérdidas, daños o accesos no autorizados a la información. Esto incluye: documentos impresos, CDs, dispositivos de almacenamiento USB y medios removibles en general.

- Recoger de forma inmediata la información sensible que se envía a las impresoras.

- Bloquear la sesión del equipo de cómputo en el momento en que se retire del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Al finalizar las actividades, se deben cerrar todas las aplicaciones y desconectar la sesión de trabajo.

- Usar el papel tapiz y el protector de pantalla corporativo, el cual se activará automáticamente después de cinco (5) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

ESTRATEGIA: EVALUACIÓN PERMANENTE DE REQUERIMIENTOS DE SEGURIDAD PARA ACTIVOS Y SOFTWARE

Políticas:

- Identificar, analizar, documentar y aprobar los requerimientos de seguridad de la información para la inclusión de un nuevo producto de hardware, software, aplicativo, desarrollo interno o externo, cambios y/o actualizaciones a los sistemas existentes en la ESU, labor que debe ser

responsabilidad del proceso de Gestión de Tecnología de la Información y de la dependencia que solicite el sistema en cuestión.

- Incluir en los acuerdos contractuales que se realicen entre la ESU y cualquier proveedor de productos y/o servicios asociados a Tecnología de la Información, los requerimientos de seguridad de la información identificados, obligaciones derivadas de las leyes de propiedad intelectual y derechos de autor.

- Garantizar la definición y cumplimiento de los requerimientos de seguridad de la Información y en conjunto con la Secretaria General establecer estos aspectos en las obligaciones contractuales específicas.

ESTRATEGIA: INTERCAMBIO SEGURO DE INFORMACIÓN

Políticas:

- Firmar acuerdos de confidencialidad con los funcionarios, clientes, proveedores y/o terceros que por diferentes razones requieran conocer o intercambiar información restringida o confidencial de la Entidad. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio seguro por cada una de las partes y se deberán firmar previamente al acceso o uso de dicha información.

- Proteger la confidencialidad e integridad de la información, teniendo especial cuidado en el uso de los diferentes medios para el intercambio de esta, que puedan generar una divulgación o modificación no autorizada.

- Para el registro de cualquier tipo de información en las bases de datos de la plataforma tecnológica de la entidad, será requisito autorizar expresamente el tratamiento de la información por parte del titular de la misma, de conformidad con la normatividad para la protección de los datos personales. En todo caso el titular de dicha información podrá solicitar su no divulgación o tratamiento por parte de la entidad, removiéndose de las bases de datos de la ESU.

ESTRATEGIA: USO EFICIENTE DE LA TELEFONÍA

Políticas:

- Realizar seguimiento y control riguroso de forma mensual frente al consumo telefónico desde las distintas extensiones habilitadas. El uso del servicio telefónico está reservado para asuntos institucionales bajo los principios de racionalidad y austeridad del gasto público.

- En términos de tiempo, las llamadas salientes y entrantes no tendrán restricción para ningún usuario.

- En términos de destino las llamadas salientes tendrán las siguientes restricciones:

    - Llamadas internacionales: Limitadas al Gerente, Secretario General y Directores.
    - Llamadas nacionales y celulares: Limitadas al Gerente, Secretario General y Directores.

- Llamadas locales: Habilitadas para todas las extensiones.

- Las llamadas nacionales, internacionales y celulares para otros usuarios, sólo se habilitarán previa solicitud del Director del área correspondiente al proceso de Gestión de Tecnología de la Información, justificando la razón y especificando el periodo de tiempo en que se deberá habilitar.

La presente resolución rige a partir de la fecha de expedición y deroga expresamente la resolución 109 de Abril 30 de 2013 y las demás disposiciones que le sean contrarias.

Dada en Medellín a los treinta (30) días del mes de Enero de dos mil quince (2015).

CÚMPLASE

MANUEL RICARDO SALGADO PINZÓN
Gerente

Aprobó: David Andres Ospina Saldarriaga - Secretario General.
Revisó: Emiro Carlos Valdez - Abogado Especialista.
Proyectó: Juliana Bermúdez Henao - Profesional Infraestructura Tecnológica.

ANEXOS

ANEXO 1
RIESGOS EN EL AREA DE GESTION DOCUMENTAL

ANEXO 2
PROGRAMA DE CONSERVACION PREVENTIVA

ANEXO 3
CRONOGRAMA DE ACTIVIDADES