

 CORANTIOQUIA	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 1 de 59

CORANTIOQUIA - Subdirección Administrativa y Financiera Medellín
RESOLUCIÓN
CORPORACIÓN AUTÓNOMA REGIONAL DEL CENTRO DE ANTIOQUIA
Fecha: 08-oct-2020 04:46 PM Pág: 5
Anexos: 54 PAGINAS
Archivar en:
Radicado por: Claudia María Gómez Londoño



Favor citar este número al responder

Por la cual se adopta la Política General de Tecnología, de Seguridad y Privacidad de la Información en la Corporación Autónoma Regional del Centro de Antioquia -CORANTIOQUIA-

La Directora General de la Corporación Autónoma Regional del Centro de Antioquia, en uso de sus facultades legales y estatutarias y en especial las que le confieren el artículo 29 de la Ley 99 de 1993 y el Decreto 1768 de 1994 y,

CONSIDERANDO

Que la Ley 1341 de 2009 estableció el marco general del sector de las Tecnologías de la Información y las Comunicaciones, incorporando principios, conceptos y competencias sobre su organización y desarrollo e igualmente señaló que las Tecnologías de la Información y las Comunicaciones deben servir al interés general y, por tanto, es deber del Estado promover su acceso eficiente y en igualdad de oportunidades a todos los habitantes del territorio nacional.

Que el Decreto Ley 019 de 2012, por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública, hace referencia al uso de medios electrónicos como elemento necesario en la optimización de los trámites ante la Administración Pública y establece en el artículo 4° que las autoridades deben incentivar el uso de las TICs a efectos de que los procesos administrativos se adelanten con diligencia, dentro de los términos legales y sin dilaciones injustificadas.

Que el Decreto 1083 de 2015, adicionado por el Decreto 415 de 2016, establece la definición de los lineamientos para el fortalecimiento institucional en materia de TICs, cuyo ámbito de aplicación, de acuerdo con el artículo 2.2.35.2., corresponde a las entidades del Estado de orden nacional y territorial, los organismos autónomos y de control.

Que el artículo 2.2.35.3. del Decreto 1083 de 2015, adicionado por el Decreto número 415 de 2016, establece como objetivos del fortalecimiento institucional:

"3. Desarrollar los lineamientos en materia tecnológica, necesarios para definir políticas, estrategias y prácticas que habiliten la gestión de la entidad y/o sector en beneficio de la prestación efectiva de sus servicios y que a su vez faciliten la gobernabilidad y gestión de las Tecnologías de la Información y las Comunicaciones TIC. Así mismo, velar por el cumplimiento y actualización de las políticas y estándares en esta materia"

...11. Desarrollar estrategias de gestión de información para garantizar la pertinencia, calidad, oportunidad, seguridad e intercambio con el fin de lograr un flujo eficiente de información disponible para el uso en la gestión y la toma de decisiones en la entidad y/o sector".

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

 CORANTIOQUIA	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 2 de 59

Que así mismo, una de las metas que pretende alcanzar el Programa Visión Colombia 2019 impulsado por el Departamento Nacional de Planeación DNP, es el cumplimiento del objetivo *"Un Estado al Servicio de los Ciudadanos"*, el desarrollo de la estrategia *"Avanzar hacia una Sociedad Informada"*, la cual dispone que: *"En 2019 la información deberá ser un derecho efectivo y un instrumento de difusión y apropiación del conocimiento, que promueva el desarrollo económico, la equidad social y la democracia. En ese contexto, Colombia deberá alcanzar estándares adecuados de generación de información confiable y oportuna, y de uso colectivo. El Estado promoverá su diseminación, aprovechando el uso de las tecnologías de la información y las comunicaciones"*, cumpliendo con los estándares de gobierno, con su nueva Política de Gobierno Digital, basada en los siguientes aspectos: TIC para lograr un Estado más eficiente, TIC para prestar mejores servicios y como herramienta para innovar en el Estado, y el nuevo enfoque hacia un Gobierno Digital.

Que mediante el Decreto 2573 de 2014, *"Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea"*, se describen los lineamientos, se incorporan mejores prácticas y se orienta la implementación para lograr una administración pública más eficiente, coordinada y transparente, a través del fortalecimiento de la gestión de las Tecnologías de la Información y se reglamenta el Marco de Referencia de Arquitectura Empresarial para Entidades del Estado, el cual es un modelo de referencia puesto a disposición del Estado colombiano para servir como orientador estratégico de las arquitecturas empresariales, lo cual debe estar articulado con los lineamientos de seguridad de la información.

Que con la transformación de la Estrategia de Gobierno en Línea a Política de Gobierno Digital, se genera un nuevo enfoque, basado en los siguiente elementos: TIC para el estado, TIC para la sociedad, Arquitectura, Seguridad y privacidad y Servicios ciudadanos digitales, en los cuales se resalta que para el diseño, estructuración y consolidación de la Política de Seguridad el logro del siguiente propósito: *"Lograr procesos internos seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información"*.

Que el Decreto 1008 de 2018 modificó el Decreto 1078 de 2018 Único Reglamentario del Sector Tecnologías de la Información y las Comunicaciones, estableciendo como cuarto componente de los elementos de la Política de Gobierno Digital, ítem 4.2 el logro de procesos internos, seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información.

Que a través del Decreto Único Reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia Gobierno Digital.

Que el Modelo de Seguridad y Privacidad de la Información (MSPI), versión 3.0.2 de julio de 2016 adoptado por el Ministerio de Tecnologías de la Información y las Comunicaciones, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 3 de 59

garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

Que para el desarrollo del componente de Seguridad y Privacidad de la Información, se ha elaborado un conjunto de documentos asociados al Modelo de Seguridad y Privacidad de la Información los cuales, a lo largo de los últimos años, han sido utilizados por las diferentes entidades tanto del orden nacional como territorial, para mejorar sus estándares de seguridad de la información.

Que CORANTIOQUIA no obstante por ser un órgano autónomo, está sujeto a las disposiciones que deben ser acogidas e implementadas en todas las entidades oficiales del orden nacional para garantizar la seguridad e integridad de la información y una adecuada gestión del riesgo.

Que por las consideraciones antes expuestas, la Directora General de la Corporación Autónoma Regional del Centro de Antioquia -CORANTIOQUIA- en mérito de lo expuesto,

RESUELVE

Artículo 1º. Objeto: Adoptar en la Corporación Autónoma Regional del Centro de Antioquia -CORANTIOQUIA-, la *Política General de Tecnología, de Seguridad y Privacidad de la Información*, como norma fundamental para el desarrollo de proyectos de tecnología con una gestión eficiente y optimización de los recursos, servicios de tecnología de información y comunicaciones y, los sistemas de información institucional.

Artículo 2º. Ámbito de Aplicación: La política aplica donde la Corporación tenga presencia o desarrollo su acompañamiento a través de la recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, en el desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos, aplicando a todas las partes interesadas de la entidad.

Artículo 3º. Sobre la Política General de Tecnología, de Seguridad y Privacidad de la Información: La Política General de Tecnología, de seguridad y Privacidad de la Información es la declaración general que representa la posición de CORANTIOQUIA, con respecto a la gestión de la tecnología y la protección de los activos de información integrados por los servidores públicos, contratistas, proveedores, la información y los procesos. Las tecnologías de información, incluido el hardware y el software que, en su conjunto, soportan los procesos de la Entidad y apoyan la implementación del esquema de Gobierno Digital y del Modelo de Seguridad y Privacidad de la Información (MSPI), por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la tecnología y la seguridad de la información.

En el marco de la presente política, CORANTIOQUIA, busca alinear la Política de Tecnología, de Seguridad y Privacidad de la Información con los instrumentos de planeación estratégica, para:

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

- Minimizar los riesgos asociados a las Tecnologías de la información y la comunicación.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los lineamientos de Gobierno Digital.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los servidores públicos, contratistas y proveedores en el manejo de la información, en las herramientas y servicios tecnológicos utilizados.
- Apoyar la innovación tecnológica.
- Implementar el Modelo de Seguridad y Privacidad de la Información (MSPI).
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de tecnología y seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y actores ambientales.
- Garantizar la continuidad de sus funciones frente a incidentes.
- Realizar acompañamiento sobre los procesos y sistemas tecnológicos para apoyar el cumplimiento de los retos estratégicos de Corantioquia y el cumplimiento del PGAR y el Plan de Acción vigente.

Artículo 4°. Nivel de Cumplimiento de la Política: Todas las partes interesadas deben dar cumplimiento a la presente política.

A continuación, se establecen las seis (6) políticas de Tecnología, de Seguridad y Privacidad de la Información en la Corporación Autónoma Regional del Centro de Antioquia -CORANTIOQUIA-:

1. Políticas Generales de TICs.
2. Políticas Administrativas.
3. Políticas de Software y Sistemas de Información.
4. Políticas de Seguridad de la información.
5. Políticas sobre Activos de Información.
6. Políticas de Hardware.

1. Políticas Generales de TICs	2. Políticas Administrativas	3. Políticas de Software y Sistemas de Información	4. Políticas de Seguridad de la Información	5. Políticas sobre Activos de Información	6. Políticas de Hardware
1.1. Aprobación sobre lineamientos y procedimientos de TI, enfocados en el sistema de gestión integral de la organización. 1.2. Alcance de los servicios de TI a nivel organizacional. 1.3. Asignación, aprobación y administración del presupuesto de TI.	2.1. Planteamiento y administración de actividades. 2.2. Adquisición de nuevas tecnologías. 2.3. Uso de equipos de computo. 2.4. Seguridad del recurso humano. 2.5. Seguridad física y del entorno. 2.6. Relaciones con los Proveedores.	3.1. Uso de licencias de software. 3.2. Instalación de software. 3.3. Acceso a servicios y plataformas de internet y correo electrónico. 3.4. Desarrollo de Software. 3.5. Adquisición, desarrollo y mantenimiento de sistemas de información.	4.1. Organización de la seguridad de la información. 4.2. Controles de Acceso. 4.3. Acceso físico al área de TI. 4.4. Seguridad de las comunicaciones y operaciones. 4.5. Gestión de incidentes de seguridad de la información. 4.6. Gestión de la continuidad tecnológica.	5.1. Gestión de Activos. 5.2. Respaldo y protección de datos e información. 5.3. Documentación 5.4. Daño o destrucción de los activos de información. 5.5. Disposiciones para protección de datos personales.	6.1. Responsabilidad de la gestión con hardware. 6.2. Disposiciones acerca de mantenimiento. 6.3. Renovación de equipos. 6.4. Operación y administración de infraestructura. 6.5. Inventario y reparación de equipos.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
 Municipio: Medellín - Antioquia
 Tel: 57 (4) 493 88 88
 Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 5 de 59

El incumplimiento a la Política General de Tecnología, de Seguridad y Privacidad de la Información en la Corporación Autónoma Regional del Centro de Antioquia -CORANTIOQUIA- traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a los lineamientos de Tecnología, Seguridad y Privacidad de la Información se refiere.

Artículo 5°. Implementación: Todas las dependencias de la Corporación Autónoma Regional del Centro de Antioquia -CORANTIOQUIA- deberán implementar la política adoptada a través del presente acto administrativo, conforme a sus responsabilidades y competencias.

Artículo 6°. Seguimiento y Revisión: La Subdirección Administrativa y Financiera o de la dependencia encargada de liderar los procesos tecnológicos de la Corporación le hará seguimiento a su implementación. La Política General de Tecnología, de Seguridad y Privacidad de la Información será revisada anualmente, o antes si existiesen modificaciones que así lo requieran, para que se mantenga oportuna, suficiente y eficaz.

Artículo 7°. Vigencia: La presente Resolución rige a partir de la fecha de su expedición y deja sin efecto cualquiera otra contraria a estas disposiciones.

Dado en Medellín, el 08 OCT 2020

PUBLÍQUESE Y CUMPLASE

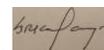


ANA LIGIA MORA MARTÍNEZ
Directora General

Anexo: Políticas Específicas de Tecnología, Seguridad y Privacidad de la Información

Elaboró: GIT TIC y GIT GIC

Revisó: Carlos Alberto Velásquez López, Gabriel Jaime Ayora Hernández.



Fecha de Elaboración: 28/08/2020

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88

Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 6 de 59

ANEXO

POLÍTICAS ESPECÍFICAS DE TECNOLOGÍA, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. POLÍTICAS GENERALES DE TICs

ALCANCE

Definir los fundamentos de Gobierno de TI para el uso de las TIC en Corantioquia. Que atienda, gestione y resuelva adecuadamente las carencias actuales y futuras, originadas en el cumplimiento de los objetivos misionales y estratégicos de la Corporación. Mediante la apropiación de conceptos como arquitectura empresarial, eficiencia, escalabilidad, calidad e innovación, que implica la participación conjunta de todos los sectores: servidores públicos, contratistas, proveedores, usuario y demás que hagan uso de las TIC en la entidad.

LINEAMIENTOS:

1.1. Aprobación sobre lineamientos y procedimientos de TI, enfocados en el sistema de gestión integral de la organización.

- La Dirección General es la responsable de la aprobación y de las disposiciones que de a lugar las políticas específicas. Los subdirectores, jefes de oficina, coordinadores y responsables de grupos internos de trabajo, deberán apoyar el propósito de adopción y cumplimiento de las políticas para toda la entidad y, fomentar la cultura del buen actuar de acuerdo a los principios institucionales.
- Los lineamientos y políticas serán en todo momento acordes con el contexto misional y visional de la Corporación, y deberán ser actualizadas y sostenidas en el tiempo.
- La entidad deberá disponer de los recursos necesario para lograr la armonía que se requiere entre el sistema de gestión integral de la Corporación con la implementación y puesta en funcionamiento de las políticas y lineamiento de los procesos tecnológicos y de seguridad de la información.
- En sintonía a las disposiciones legales, normativas y que tienen jurisdicción para Corantioquia, esta adoptará las políticas que garanticen en todo momento la disponibilidad, confidencialidad e integridad de la información y de los sistemas que le procesan.

1.2. Alcance de los servicios de TI a nivel organizacional.

- Para generar una eficiente y efectiva comunicación en dos vías con la comunidad, Corantioquia dispone de recursos tecnológicos y personal capacitado de manera que se logre los objetivos institucionales. Esto dentro del marco de la gestión pública y relacionamiento con el Estado.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 7 de 59

- El Área de TICs en conjunto con todas las dependencias de la entidad, creará un listado de servicios los cuales hará públicos en la página web de la Corporación y, los mantendrá actualizados de cara a la ciudadanía.
- Las funciones propias del Área de TICs que se consideren servicios a otras dependencias, serán solicitados de manera formal mediante correo electrónico.

1.3. Asignación, aprobación y administración del presupuesto de TI.

- La Corporación mediante el PGAR, define los lineamientos que debe seguir la corporación en materia ambiental, ese plan debe detallarse cada cuatro años en el Plan de Acción y el área de tecnología debe participar en la construcción de los mismos. El Plan de Acción debe soportarse sobre un Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETICO, que debe seguir la corporación y definir un presupuesto que se ejecutará de manera anual atendiendo las prioridades y enfoques que la dirección quiera darle.
- La dependencia que lidere los procesos tecnológicos de la Corporación, de manera anual, presentará el presupuesto que usará durante la vigencia, con la priorización de proyectos y asuntos necesarios para administrar de manera adecuada y generar valor a las diferentes áreas y procesos de la organización.
- La dependencia que lidere los procesos tecnológicos de la Corporación dentro de sus responsabilidades estará el de planear, organizar, coordinar, realizar e inspeccionar el presupuesto, proyectos e inversiones de las Tecnologías de la Información y las Comunicaciones - TIC para la Entidad.
- La dependencia que lidere los procesos tecnológicos de la Corporación tendrá la responsabilidad de definir, emprender y ejecutar los presupuestos que Corantioquia establezca para la gestión - TIC.
- Las Subdirecciones Administrativa y Financiera, y de Planeación, proveerán a la dependencia que lidere los procesos tecnológicos de la Corporación, soporte logístico, talento humano, recursos materiales, presupuestales y todos los necesarios para el correcto cumplimiento de las obligaciones.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 8 de 59

2. POLÍTICAS ADMINISTRATIVAS

ALCANCE

Establecer directrices, lineamientos y políticas que permitan a Corantioquia contar con el marco de gestión en procesos tecnológicos y de seguridad de la información acordes a la estrategia que desea implementar de cara al futuro. Propiciando el mejor desarrollo de las actividades y asegurando la provisión oportuna a las condiciones necesarias para la obtención de grandes resultados.

LINEAMIENTOS:

2.1. Planteamiento y administración de actividades.

- El Área de TICs creará, mantendrá y gestionará un plan estratégico para cada cuatro (4) años que marcará la ruta de su gestión y donde se alineará a los objetivos y retos estratégicos de la Corporación.
- Para proyectos que impliquen desarrollo de software, se dispondrá de los lineamientos en relación a éste y disponibles en las políticas de software y sistemas de información (numeral 3.4.). Estos deben ser coordinados con la dependencia que lidere los procesos tecnológicos de la Corporación.

2.2. Adquisición de nuevas tecnologías.

- La dependencia que lidere los procesos tecnológicos de la Corporación, será la encargada de valorar y recomendar la compra u obtención de los recursos informáticos para cualquier área de la entidad.
- La dependencia que lidere los procesos tecnológicos de la Corporación, proveerá su concepto para la adquisición de recursos a nivel de hardware, software y otros dispositivos electrónicos, concepto emitido con sustento en calidad, respaldo y reconocimiento en el mercado.
- Todas las particularidades de tecnología y las propuestas con mejor aceptación técnica, será definida por la dependencia que lidere los procesos tecnológicos de la Corporación, quien adelantará labores de asesoría y colaboración para adquisición de nuevos recursos tecnológicos e informáticos.
- La dependencia que lidere los procesos tecnológicos de la Corporación, aportará el concepto y las definiciones a modo de precepto para los aspectos de compra y adquisiciones tecnológicas e informáticas de acuerdo a la importancia y conforme a la peculiaridad de cada caso.
- Cuando las dependencias adquieran nuevas tecnologías, La dependencia que lidere los procesos tecnológicos de la Corporación, asumirá la responsabilidad de su mantenimiento.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 9 de 59

- La dependencia que lidere los procesos tecnológicos de la Corporación, participará en el comité de contratación para apoyar adquisiciones en materia de TICs.

2.3. Uso de equipos de cómputo.

- Todo usuario que haga uso de cualquier herramienta tecnológica o tenga bajo su responsabilidad equipo de cómputo propiedad de la Corporación se compromete a hacer uso responsable y exclusivo de este sólo para sus actividades laborales.
- Corantioquia pone a disposición de los usuarios equipos de cómputo, herramientas tecnológicas, entre otros, para el cumplimiento de sus funciones. Por tanto, el usuario debe abstenerse de hacer uso de dichas herramientas e información para propósitos personales o fines lucrativos. El uso será sólo para lograr los objetivos de la Corporación.
- Cada usuario velará por la limpieza y buen estado de su equipo de cómputo o herramienta tecnológica. No debe preparar ni consumir alimentos o bebidas sobre el o su entorno, para evitar afectaciones en el funcionamiento de las actividades y disponibilidad de los recursos.
- De causarse daño por mala utilización o descuido sobre el equipo de cómputo o herramienta tecnológica por parte del usuario, este asumirá el costo de reparación o cambio sin que se le sancione disciplinariamente, para ello se hará un procedimiento administrativo a cargo de talento humano.
- Después de la entrega del equipo de cómputo de parte la dependencia que lidere los procesos tecnológicos de la Corporación al usuario, este se hace responsable y debe seguir las disposiciones normativas para su utilización. En caso de encontrarse software ilegal, no autorizado o de contrabando, el usuario asumirá las sanciones que den a lugar.
- No esta permitido emplear el equipo de cómputo para descargar juegos, música, videos, imágenes, fotos, protectores de pantalla, archivos de fuentes no seguras o contenidos que hiera o afecte sensibilidades y que incumplan la normatividad colombiana.
- Los usuarios deberán advertir a sus jefes inmediatos si se presenta, con recurrencia, situaciones de fallas en los equipos o sistema eléctrico o reducciones de voltaje con el fin de que sea notificado a la dependencia que lidere los procesos tecnológicos de la Corporación y desde allí se tome las medidas preventivas o correctivas necesarias.
- El usuario esta en la obligación de revisar que el antivirus este actualizado y, de examinar cualquier dispositivo que se inserte en el equipo; en caso que esta desactualizado o presente alguna anomalía, deberá informar de la situación a la dependencia que lidere los procesos tecnológicos de la Corporación.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 10 de 59

- Los usuarios deberán dar el uso adecuado a las herramientas tecnológicas requeridas para el uso de sus funciones, procurando tener los saberes necesarios en el manejo de hardware y software que se requiera. Así mismo, los usuarios deberán acogerse a los procedimientos e indicaciones definidas por la dependencia que lidere los procesos tecnológicos de la Corporación para salvaguardar la disponibilidad e integridad de la información.
- Si el usuario requiere conectarse a la red con un equipo diferente, deberá solicitar autorización a la dependencia que lidere los procesos tecnológicos de la Corporación y seguir el procedimiento dispuesto para ello con la autorización del jefe de área.
- Todos los equipos de cómputo, equipos de telecomunicaciones, artefactos tecnológicos entre otros bienes propiedad de Corantioquia son de su pertenencia, por tanto la información que allí se procese, almacene o gestione, también.
- Los usuarios no podrán cambiar las firmas de correo electrónico, fotos de cuenta de red, fondos de pantalla, estos serán establecidos por la Oficina de Comunicaciones y administrados por la dependencia que lidere los procesos tecnológicos de la Corporación.

2.4. Seguridad del recurso humano.

Asegurar que todos los servidores públicos, contratistas, proveedores y/o terceros entiendan sus responsabilidades y sean conscientes sobre la seguridad de la información y su importancia dentro de la Entidad. Asegurar un ciclo laboral con transiciones seguras minimizando el riesgo de fuga de información.

2.4.1. Sobre la relación laboral en materia de seguridad de la información.

- Los servidores públicos, contratistas, proveedores y/o terceros con acceso a los activos de información de Corantioquia deben conocer, entender y seguir la política general y las políticas específicas de seguridad de la información de la Entidad.
- Todos los servidores públicos, contratistas, proveedores y/o terceros deben informar acerca de los eventos que atenten contra la seguridad de la información de Corantioquia, así como los eventos potenciales u otros riesgos que sean de su conocimiento.
- El Grupo Interno de Trabajo de Talento Humano debe asegurar que cada funcionario reciba una inducción sobre las Políticas Generales de Tecnología, Seguridad y privacidad de la Información.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 11 de 59

- Con el objetivo de mantener actualizadas las funciones de los funcionarios sobre Seguridad de la información, el Grupo Interno de Trabajo de Talento Humano, en sinergia con cada jefe, deberá garantizar el ajuste de funciones de acuerdo con los cambios que se presenten en la Corporación.

2.5. Seguridad física y del entorno.

Minimizar los riesgos potenciales que puedan resultar en pérdida de información por robo o daño a los recursos informáticos, de manera accidental o por accesos no autorizados.

2.5.1. Escritorio seguro y pantalla limpia.

- Ningún usuario debe tener información confidencial de la Entidad en su puesto de trabajo, ni escrita en lugares visibles o fácilmente accesibles. Deben mantener su escritorio limpio y con la información bien almacenada. Deben mantener presente no publicar o dejar a la vista, documentos o datos sensibles, como por ejemplo:
 - Nombre de Usuario y contraseña.
 - Direcciones IP e información sobre la plataforma informática de Corantioquia.
 - Números de cuenta bancaria.
 - Propiedad Intelectual.
 - Información privada de personas naturales y/o jurídicas.
 - Cualquier activo clasificado como no público.
 - Las claves deben ser personales e intrasferibles.
- Cada funcionario, contratista, proveedor y/o tercero debe garantizar que los sistemas de información y elementos de procesamiento utilizados deben estar adecuadamente protegidos, teniendo presente que se debe guardar documentos confidenciales.
- Cada usuario debe asegurar que su computador o estación de trabajo no quede desatendida. Cuando el usuario no esté al frente de su estación de trabajo esta debe quedar bloqueada con el fin de evitar suplantación de identidad, ya que cada persona es responsable por lo que se haga con su usuario personal.

2.5.2. Áreas de acceso restringido.

- El acceso a las áreas restringidas donde se desarrollen actividades de Tecnología, será autorizado por el Coordinador o Jefe de la dependencia que lidere los procesos tecnológicos de la Corporación y, en todo caso se guardará los protocolos de seguridad, eso incluye que personal externo sea acompañado permanentemente.
- En las instalaciones de Corantioquia, se deben identificar áreas especiales que mantienen recursos de información o instalaciones sensibles o críticas para las operaciones diarias de la Entidad. Estas

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
 Municipio: Medellín - Antioquia
 Tel: 57 (4) 493 88 88
 Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 12 de 59

áreas deben mantener controles de acceso adecuados para su protección.

- El acceso a áreas seguras debe realizarse desde áreas internas. No deben tener forma de acceso desde el exterior.
- Cada una de las áreas de acceso restringido debe tener identificado formalmente un responsable de la misma, en el caso del centro de cómputo principal el responsable es la dependencia que lidere los procesos tecnológicos de la Corporación.
- Los responsables de cualquier tipo de área controlada tienen que mantener controles de acceso efectivos, en proporción a los recursos humanos y al valor de los activos a proteger.

2.5.3. Protección de los equipos de cómputo.

- Se deberán establecer procedimientos de ingreso, transporte, movimiento, eliminación y retiro de los recursos tecnológicos.
- Se debe garantizar la disponibilidad de los recursos y servicios necesarios para la adecuada operación de los recursos tecnológicos que soportan la información de Corantioquia. (Por ejemplo: suministros de energía eléctrica, condiciones ambientales, control de acceso, entre otras).
- Se deben establecer las acciones necesarias para coordinar, apoyar, capacitar y responder frente a eventos o escenarios catastróficos que puedan afectar a las personas que laboran en la Entidad, así como los activos y medios que permiten procesar la información de la misma. Esta información debe ser incluida en el Sistema de Gestión Integral y apoyada por Talento Humano.
- Antes de ingresar equipos a los centros de cómputo, se deben identificar al menos los siguientes requerimientos con el fin de tomar decisiones de acuerdo con lo que puede ofrecer el centro de cómputo y no afectar a los demás equipos allí ubicados:
 - Consumo de potencia.
 - Carga calórica generada.
 - Características de temperatura soportadas.
 - Área ocupada (Dimensiones).
- Los dispositivos de almacenamiento con información sensible deberán ser destruidos una vez su vida útil haya finalizado, esto deberá estar enmarcado en un programa de renovación y actualización tecnológica ejecutado por el Coordinador o Jefe de la dependencia que lidere los procesos tecnológicos de la Corporación, con el fin de no conservar medios obsoletos que contengan información confidencial o sensible.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

 CORANTIOQUIA	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 13 de 59

- En el caso de terminar la vida útil de un equipo, ya sea por daño o porque se encuentra enmarcado en un proceso de renovación tecnológica, la información que este posea deberá ser des truida a través de mecanismos seguros, tales como equipos de desmagnetización para discos, herramientas de sobre-escritura de información, borrado a bajo nivel, y otros. Estas herramientas deben ser aprobadas por el Coordinador o Jefe de la dependencia que lidere los procesos tenológicos de la Corporación y utilizada por el personal de asistencia.
- En prácticas de arrendamiento de equipos, se deberán aplicar las medidas de borrado seguro de información de estos una vez se termine el periodo de alquiler. Estos elementos deberán ser contenidos en el procedimiento de devolución de equipos.

2.5.4. Mantenimiento de equipos.

- El mantenimiento de equipos deberá realizarse en una zona especial definida para este fin, manteniendo las características de control de acceso y seguridad de los equipos de acuerdo con la información que estos soportan.
- El equipo de trabajo del Coordinador o Jefe de la dependencia que lidere los procesos tenológicos de la Corporación planeará el mantenimiento de equipos de cómputo de manera periódica en la sede central y las sedes de oficinas territoriales.
- Se deberán tener procedimientos de mantenimiento documentados para los equipos de cómputo. Tanto para equipos servidores como para estaciones de trabajo.
- Para los equipos que por labores de mantenimiento deban ser llevados fuera de las instalaciones de Corantioquia, deberán establecerse medidas de control para evitar que la información sensible contenida sea divulgada. Por esta razón, la información contenida en estos, deberá ser retirada o, protegida, de los dispositivos, con el fin de evitar que personal externo tenga acceso a la misma o pueda ser copiada. Estos elementos deberán estar contenidos en los procedimientos de mantenimientos de equipos.
- Cada equipo de cómputo debe contar con su respectiva hoja de vida, donde se registre la bitácora de los mantenimientos preventivos y correctivos efectuados.

2.5.5. Centro de cómputo.

- La dependencia que lidere los procesos tenológicos de la Corporación tiene la obligación de definir los requerimientos de seguridad física necesarios para los componentes tecnológicos en los centros de cómputo, almacenamiento, procesamiento y telecomunicaciones.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 14 de 59

- El acceso al Centro de cómputo, será autorizado por el Coordinador o Jefe de la dependencia que lidere los procesos tecnológicos de la Corporación y, en todo caso se guardará los protocolos de seguridad, eso incluye que personal externo sea acompañado permanentemente.
- Se debe elaborar un diseño detallado de los mecanismos de restricción de acceso físico, cuya administración permita un registro de los accesos tanto de personal autorizado como de visitantes.
- Se debe desarrollar una evaluación de riesgos de los activos informáticos ubicados en centros de cómputo, procesamiento y telecomunicaciones, que permita establecer el riesgo y los controles necesarios para mitigarlos
- Se deben incluir todos los controles mínimos ambientales que permitan proteger los componentes frente a riesgos ambientales como fuego y agua y aquellos de suministro de energía y aire, de acuerdo al análisis de riesgos definido.
- El personal externo que requiera desempeñar labores en el centro de cómputo ó centros de cableado ubicados en las instalaciones de la Sede Central, debe permanecer acompañado en todo momento por una persona designada por la dependencia que lidere los procesos tecnológicos de la Corporación.
- Se debe elaborar una política específica de acceso al centro de cómputo, donde se definan los procedimientos de ingreso, los cuidados que se deben tener, las obligaciones de cada persona que ingresa y las políticas que debe respetar.
- Las labores de mantenimiento y aseo de estos centros deberá estar sujeto a un procedimiento formal, donde se indique en qué puntos se pueden conectar equipos de aseo, como se maneja el material de limpieza y como se debe registrar la persona que realiza el aseo.
- Se deben verificar los riesgos potenciales que tienen este tipo de trabajos e informarlos a los responsables del centro de cómputo para que tomen las medidas necesarias para evitar daños en los equipos.

2.5.6. Sistema de respaldo eléctrico.

- El centro de cómputo debe tener generador de respaldo (planta eléctrica autónoma) y poseer un sistema redundante de respaldo (de ser posible).
- El centro de cómputo debe tener un sistema ininterrumpido de potencia (UPS) de respaldo y se deben realizar revisiones periódicas para el mantenimiento y revisión de vida útil de las baterías de la UPS.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

 CORANTIOQUIA	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 15 de 59

- El centro de cómputo debe tener sistema de aire acondicionado acorde a las necesidades de flujos de aire y temperaturas de acuerdo a las especificaciones de los equipos, este sistema debe contar con mecanismos de apagado automático en caso de incendios. Se deberá realizar una evaluación anual sobre las condiciones ambientales y de temperatura de estos centros (Cómputo y Cableado).
- El centro de cómputo debe tener un sistema de tierra independiente.
- El centro de cómputo debe mantener actualizado un plano de conexiones eléctricas de todos los equipos y las tomas eléctricas deberán encontrarse identificadas.
- El centro de cómputo debe tener sistema de alumbrado automático de manera que cuando en el centro no se encuentren personas, permanezca apagado.
- El centro de datos, respaldo de seguridad y backup deberán contar con un plan de recuperación ante la eventualidad de desastres.

2.5.7. Ubicación de equipos.

- Se deberá mantener un inventario de los equipos ubicados en cada uno de los centros de cómputo y de cableado de Corantioquia.
- Se deberá tener en cuenta la correcta ubicación para garantizar la correcta disipación de calor de los equipos.
- Se deben realizar periódicamente estudios de temperaturas en los centros de cómputo donde se encuentran almacenados los equipos.

2.5.8. Aire acondicionado.

- Deberá disponerse de los equipos de aire acondicionado necesarios (por lo menos dos para proveer respaldo) para mantener la temperatura y la humedad adecuadas para los equipos.
- Se deben hacer revisiones periódicas sobre los equipos de aire para evitar problemas relacionados con la condensación del aire, goteos de agua, por lo tanto se deberá tener especial cuidado en los drenajes necesarios cerca de estos.
- Los aires acondicionados deben conectarse a los sistemas eléctricos de emergencia (planta eléctrica), pues en caso de un corte en la electricidad, este servicio no puede suspenderse sin el consecuente daño a los equipos.
- Los aires acondicionados deberán poseer sistemas de automatización de arranque y de respaldo.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 16 de 59

- El centro de cómputo deberá tener adecuados detectores de temperatura y humedad y un registro histórico de estas variables.

2.5.9. Sistema de detección y extinción de incendios.

- Todo centro de cómputo deberá tener detectores de incendio adecuados y deberá seguir a la norma de la NFPA (National Fire Protection Association) NFPA 75: Protección de equipos electrónicos procesadores de datos por computador Referencia: XE 75 92E.
- Las puertas de salida de emergencia, los detectores de incendio, los sistemas de alarma visual y auditiva y los procedimientos de activación y desactivación de los sistemas deberán ensayarse al menos cada dos meses para comprobar su correcto funcionamiento (en caso de tenerlos).
- Deberá tenerse una señalización adecuada de todos estos elementos.

2.5.10. Mantenimiento.

- Todos los equipos necesarios para el adecuado funcionamiento del centro de cómputo deberán estar amparados con contratos de mantenimiento preventivo y correctivo. La dependencia que lidere los procesos tecnológicos de la Corporación deberá coordinar junto con el Grupo Interno de Trabajo de Recursos Físicos las actividades de mantenimientos mediante la programación anual de mantenimientos sobre los equipos de cómputo, los controles ambientales y de protección contra fuego, detección de humedad, plantas eléctricas, UPS, entre otros.

2.6. Relaciones con los Proveedores.

Establecer parámetros de contratación de terceros respecto a la seguridad de la información y su compromiso con la misma, definir la responsabilidad del gestor del contrato sobre la asignación y revocación de privilegios para los terceros y establecer directrices especiales que se deben tener en cuanto a la seguridad de la información cuando personas externas a Corantioquia utilizan los recursos de la Entidad.

2.6.1. Computadores de contratistas, proveedores y/o terceros conectados a la red.

- En los contratos o acuerdos con contratistas, proveedores y/o terceros se debe incluir una cláusula o acuerdo de confidencialidad y no divulgación, donde se establezca la responsabilidad en cuanto al uso de la información propiedad de Corantioquia y al cumplimiento de la política general y las políticas específicas de seguridad de la Entidad. También debe incluir las consecuencias por el incumplimiento a cualquiera de estas dos.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 17 de 59

- Se debe contar con un software tipo NAC (Network Access Control) que controle el acceso a la red por parte de contratistas, proveedores, terceros y personal invitado.
- El funcionario que facilite o permita la conexión de un equipo externo a la red corporativa, sin la autorización de la dependencia que lidere los procesos tecnológicos de la Corporación, asumirá las consecuencias que pudieran presentarse ante un incidente de seguridad y las sanciones disciplinarias a las que hubiera lugar.
- Por seguridad los equipos de cómputo para conectarse a la red de la Entidad, de todo contratista, proveedor y/o tercero deben , tener instalado y actualizado un antivirus, así mismo, el sistema operativo actualizado.
- En el caso de servicios de outsourcing y contratos de prestación de servicios, que utilicen equipos que están en la red de Corantioquia de forma permanente, el contratista, proveedor y/o tercero deberá enviar anualmente un certificado en el que garantice que las licencias de software de su propiedad que están siendo usadas en dichos equipos, fueron legalmente adquiridas y/o actualizadas.
- Los equipos de contratistas, proveedores y/o terceros que se conectan regularmente a la red de Corantioquia deben someterse periódicamente al chequeo básico de seguridad informático definido por la Entidad.
- Las personas que realicen visitas esporádicas a Corantioquia podrán solicitar el servicio de Internet de Invitados. Esta red debe estar separada lógicamente de la red de la Entidad y no debe tener acceso a ningún recurso interno.
- La red de invitados debe ser utilizada exclusivamente por las personas a quien está destinada (invitados), en ningún momento debe ser usada por servidores públicos, contratistas, proveedores y/o terceros, los cuales deben usar las redes inalámbricas que tienen asignadas.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 18 de 59

3. POLÍTICAS DE SOFTWARE Y SISTEMAS DE INFORMACIÓN

ALCANCE

Adoptar políticas que operen dentro del marco legal (De conformidad a la Ley 1915 del 12 de julio de 2018, Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derechos de autor y derechos conexos) para prevenir y contener el uso ilegal de software en la Corporación. Entendiéndose que cualquier equipo de la entidad que posea un software deberá ser licenciado, de lo contrario será ilegal y tendrá que ser eliminado. Igualmente, la creación de programas de cómputo deberá cumplir con las condiciones de ley en materia de su desarrollo e implementación.

LINEAMIENTOS:

3.1. Uso de licencias de software.

- De conformidad a la Ley 1915 del 12 de julio de 2018 “por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos”, Corantioquia garantiza que todo software utilizado en los equipos de cómputo de su jurisdicción es licenciado, en caso contrario dicho software será eliminado de manera inmediata.
- Será la dependencia que lidere los procesos tecnológicos de la Corporación encargada de gestionar y administrar las licencias de software de los equipos de la Corporación. Asegurando que se dispongan de la mejor manera y a los usuarios que la requieren.
- La dependencia que lidere los procesos tecnológicos de la Corporación debe llevar un registro actualizado de las licencias de software, su valor, distribución y fecha de expiración, relacionando la funcionalidad y el área o personal encargado, con el fin de mantener optimizado el uso de las mismas. La correcta gestión del registro actualizado permitirá a la Corporación una gestión eficaz de costos y asegurar el cumplimiento ante una auditoría sobre las licencias de software, ya sea por parte del proveedor o interno en la Corporación.
- Queda prohibido el uso de licencias en la instalación de software para equipo que no sean propiedad de Corantioquia. Salvo situaciones de índole especiales y previa autorización del Líder de la dependencia que lidere los procesos tecnológicos de la Corporación.
- La Subdirección Administrativa y Financiera dispondrá de los presupuestos para la adquisición de licencias de software a fin que la Corporación siempre cumpla con la ley de derechos de autor y legalidad en los equipos.
- Será responsabilidad de la dependencia que lidere los procesos tecnológicos de la Corporación suprimir cualquier software que no posea licencia y que pueda ocasionar sanciones económicas y judiciales a la entidad. Además llevará un registro de éstos software para efectos de

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88

Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 19 de 59

analítica y verificar reincidencia, de manera que se pueda establecer responsabilidades y sanciones disciplinarias que de a lugar por parte de la Oficina de Control Interno Disciplinario. En todo caso, el personal de la dependencia que lidere los procesos tecnológicos de la Corporación deberá actuar con prudencia y cuidado de la privacidad del usuario, indicándole el procedimiento a seguir y logrando su aprobación para la gestión a realizar.

- Los recursos originales para realizar las instalaciones, acceso a portales, llaves de instalación, entre otras, será responsabilidad de la dependencia que lidere los procesos tecnológicos de la Corporación, quien en todo momento hará custodia y administración de estos.

3.2. Instalación de software.

- Sólo está autorizado el personal de la dependencia que lidere los procesos tecnológicos de la Corporación para la instalación de software en los equipos de cómputo de la Corporación.
- Queda prohibido la instalación de cualquier tipo de software por parte de los usuarios en sus equipos de cómputo. Todo requerimiento de instalación será canalizado por la dependencia que lidere los procesos tecnológicos de la Corporación.
- El Líder de la dependencia que lidere los procesos tecnológicos de la Corporación aprobará y autorizará la instalación de software en los equipos con su respectiva licencia.
- Esta prohibido instalar software de propiedad de Corantioquia en equipos que no sean suyos.
- La dependencia que lidere los procesos tecnológicos de la Corporación deberá llevar un registro con todos los software y programas que se encuentren instalados en los equipos de cómputos de la entidad y, deberá actualizarse al menos cada año.
- La dependencia que lidere los procesos tecnológicos de la Corporación deberá garantizar la seguridad necesaria desde el sistema operativo del equipo, hasta el software final empleado para el acceso a la información.
- La dependencia que lidere los procesos tecnológicos de la Corporación será la encargada de planear, administrar y ejecutar las actualizaciones de nuevos versionamientos de software para los equipos de la Corporación, esto incluye parches de seguridad, actualización de bios, actualizaciones a software de gestión, y en general, todas las actualizaciones necesarias para el correcto funcionamiento de los sistemas de información de la Corporación.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 20 de 59

- Queda prohibido el uso de software o programas que no requieran instalación y que para su funcionamiento estén alojados en memorias USB, discos duros portables, dispositivos de entrada, u otro medio para tales fines.
- Cualquier software o programa que el usuario requiera para sus labores y que podría descargarse e instalarse desde algún sitio web, deberá ser solicitado formalmente a la dependencia que lidere los procesos tecnológicos de la Corporación con su justificación y aprobación del Líder del área. Esto con el propósito que no se vulnere la seguridad de la entidad y que el criterio de instalación sea aprobado desde la competencia y criterio de la dependencia que lidere los procesos tecnológicos de la Corporación.

3.3. Acceso a servicios y plataformas de internet y correo electrónico.

- La dependencia que lidere los procesos tecnológicos de la Corporación será la administradora de los servicios de internet y correo electrónico para la Corporación. Cualquier requerimiento en relación a éstos deberá canalizarse por esta.
- Toda comunicación en el ámbito y ejercicio de las actividades laborales, deberá ser mediante los canales institucionales como las cuentas de correo electrónico con dominio <nombre de usuario>@corantioquia.gov.co.
- Tanto la disponibilidad de la infraestructura tecnológica, como el acceso a las plataformas, servicios de internet, correo electrónico y otras utilidades online, deberán contar con una disponibilidad bajo condiciones optimas que permita el correcto desarrollo de las actividades de la Corporación.
- Cada usuario que disponga de una cuenta de correo electrónico, será responsable de su uso, advirtiéndose que por tratarse de una cuenta institucional, deberá hacer uso exclusivo para intercambio oficial de información en relación a sus funciones y, abstenerse de hacer uso personal de esta.
- El uso de las plataformas, utilidades online, servicio de internet, correo electrónico y demás a las que disponga el usuario en los equipos de la Corporación, será para uso único y exclusivo de sus funciones contractuales, en ningún caso deberá hacer uso de éstos para temas personales u otros fines no autorizados.
- La dependencia que lidere los procesos tecnológicos de la Corporación asignará cuentas de correo y acceso a las plataformas conforme a la disponibilidad que haya y a los procedimientos establecidos para tal fin.
- Queda prohibido prestar, regalar, facilitar, proporcionar u ofrecer cuentas de correo o acceso a terceras personas.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 21 de 59

- Será deber de la dependencia que lidere los procesos tecnológicos de la Corporación mantener el servidor de correo y el firewall Corporativo actualizado y protegido contra virus, en especial para correos entrantes y correos salientes.
- Esta prohibido hacer mal uso del correo institucional mediante cadenas de mensajes, envío de mensajes masivos o spam. El usuario deberá evitar estas acciones para protegerse y evitar extender algún virus en los sistemas de la Corporación.
- Todo usuario deberá abstenerse de abrir correos electrónicos de dudosa procedencia, en tal caso deberá marcarlo como spam y eliminarlo, notificando a la dependencia que lidere los procesos tecnológicos de la Corporación sobre la situación presentada.
- Todo usuario deberá evitar dar a conocer su cuenta de correo institucional a personas o entes que no sea conocidos o que tengan dudosa procedencia.
- Ningún equipo que esté designado como servidor debe tener asociada una cuenta de correo electrónico.
- En todo caso, los mensajes de correo electrónico se regirán por los lineamientos norma de urbanidad y civismo, no se deberá emplear lenguaje inapropiado, desobligante e inmoral, sino que se deberá conservar el respeto y amabilidad debido a que se trata de documentos formales.
- Al enviar un correo electrónico se deberá considerar siempre:
 - Adicionar un asunto que enmarque el objeto del mensaje.
 - Ser conciso, cordial y respetuoso en el mensaje.
 - Adjuntar solo lo necesario e indispensable.
 - No enviar mensajes a todas las cuentas de la corporación, a no ser que sea autorizado por el Jefe inmediato.
 - Si se requiere enviar mensajes masivos, se debe usar listas de distribución y la opción de “copia oculta” Bcc o Cco en lista de destinatarios o solicitar al área de Comunicaciones dicha gestión.
- En envió de mensajes de interés general como actividades, convivencias, invitaciones, entre otras, deberá ser enviadas por el área de Comunicaciones de la Corporación.
- Los usuarios deberán eliminar periódicamente los mensajes que no sean relevantes, necesarios e importantes para sus funciones.
- Será el área de Talento Humano quien notifique o solicite a la dependencia que lidere los procesos tecnológicos de la Corporación, la

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 22 de 59

creación, eliminación o inhabilidad de una cuenta de correo electrónico, de acuerdo a los procesos de gestión de accesos.

- Es responsabilidad de todos los usuarios propender por la seguridad en su estación de trabajo, para lo cual deberá estar atento a las notificaciones de actualización de antivirus e informar novedades desfavorables la dependencia que lidere los procesos tecnológicos de la Corporación cuando se presente alguna.
- Será la dependencia que lidere los procesos tecnológicos de la Corporación quien dará las indicaciones para las configuraciones de seguridad como: certificados de navegadores, cookies entre otros, los cuales no podrán ser alterados salvo autorización de la dependencia que lidere los procesos tecnológicos de la Corporación.
- Esta prohibido hacer uso de la herramienta de correo electrónico o servicios de nube para:
 - Ofrecer productos o servicios.
 - Hacer propaganda política.
 - Hacer campañas publicitarias.
 - Enviar cadenas o información externa a la Corporación.
 - Insultar, denigrar, amenazar, difamar o desprestigiar personas naturales o jurídicas.
 - Promulgar la invitación para seguir a alguien en redes sociales.
 - Promulgar la invitación a suscribirse a boletines electrónicos, sitios web, periódicos, revistas, seminarios, buscadores de parejas o cualquier otro que no vaya en función de la profesionalidad del usuario.
 - Descargar o compartir archivos personales, música, software, videos, imágenes y cualquier otro que no guarde estricta relación con el área profesional del usuario.
 - Incumplir cualquier disposición en materia legal y normativa.
 - Transferir información sin autorización.
- La dependencia que lidere los procesos tecnológicos de la Corporación tomará las acciones necesarias (por medio de software especializados u otros medios) para garantizar que ninguna de las situaciones anteriores se presenten en el entidad y, evitar así, el acceso no autorizado y mal utilización de los recursos institucionales.

3.4. Desarrollo de Software.

3.4.1. Política general de desarrollo de software.

- La dependencia que lidere los procesos tecnológicos de la Corporación debe definir procedimientos de desarrollo de software , acordes a las practicas del campo, estimando los recursos y el tiempo para los tipos de desarrollo de software de la Corporación. Deberá además, contar con disposiciones especiales para la atención de situaciones donde el sistema misional de la entidad lo requiera debido al impacto o criticidad sobre esta.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

 CORANTIOQUIA	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 23 de 59

- El área de desarrollo deberá analizar el argumento y, valorar la viabilidad a las solicitudes para creación o modificación de algún sistema.
- La homologación y promoción de herramientas que apoyen los proyectos de desarrollo, adaptados con las mejores metodologías y en cumplimiento a los requisitos mínimos de control, deberán ser direccionados y adaptados por el área de desarrollo.
- Será responsabilidad del área de desarrollo la homologación de cualquier nuevo software para proyectos de TI de cualquier dependencia de la Corporación.
- Desde la dependencia que lidere los procesos tecnológicos de la Corporación en conjunto con el área de desarrollo se deberá desarrollar temas como:
 - Formación y capacitación para el equipo de desarrollo.
 - Pruebas de software funcionales, no funcionales, estructurales, de regresión y re-prueba.
 - Desarrollo para móviles.
 - Seguridad del desarrollo del software.
 - Base de datos.
 - Ingeniería del software.
 - Elicitación de requisitos y casos de uso
 - Análisis computacional de datos
 - Diseño UX/IU (Experiencia de usuario / Interfaz de usuario) y línea gráfica.

3.4.2. Admisión de solicitudes para desarrollo de software.

- Cualquier proyecto, creación o modificación de sistema, debe apegarse a los procedimientos y tiempos determinados por el área de desarrollo para la atención del mismo.
- Toda solicitud para nuevos desarrollos o modificaciones a existentes, debe formalizarse mediante solicitud de creación o modificación de sistema.
- Las solicitudes de creación o modificación de sistema deberán ser firmadas por el jefe de dependencia solicitante y, tendrá que ser aprobada por la dependencia que lidere los procesos tecnológicos de la Corporación antes de cualquier boceto preliminar.

3.4.3. Asignación de recursos económicos, talento humano y materiales.

- El área de desarrollo proveerá el talento humano conforme al perfil requerido para el proyecto, ajustándose a los procesos de selección y contratación que apliquen en la Corporación.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 24 de 59

- Si algún proyecto requiere de servicios tercerizados y/o la adquisición de bienes informáticos u otros, la dependencia solicitante asumirá los costos de estos conforme a la normatividad y procedimientos establecidos por la entidad.

3.4.4. Manejo de estándares y documentación.

- El área de desarrollo definirá una o dos metodologías, según sea el caso del proyecto, definiendo los elementos requeridos durante el ciclo de vida del desarrollo.
- El área de desarrollo definirá la metodología para documentar y garantizar el ciclo de vida del desarrollo.
- El área de desarrollo definirá la guía para nombrar los objetos de la base de datos, considerando buenas prácticas en codificación de procedimientos y sentencias.
- Desde la dependencia que lidere los procesos tecnológicos de la Corporación se proveerá criterio y vigilará la aplicación de las metodologías y estándares para el desarrollo de software y el intercambio de información entre entidades del estado, esto en conjunto con el área de desarrollo.

3.4.5. Contratación y control de personal externo y servicios tercerizados.

- Es competencia de la dependencia que lidere los procesos tecnológicos de la Corporación asegurar que:
 - Se de cumplimiento fiel y fidedigno al contrato, el cual deberá estar avalado por su respectiva normatividad para efectos de legalidad.
 - Toda tercera parte que intervenga en el proyecto como contratista o proveedor de servicio, tendrá al menos que cumplir con requisitos que se exige para el personal de la dependencia que lidere los procesos tecnológicos de la Corporación.
 - De acuerdo a las condiciones del pago del servicio, la dependencia que lidere los procesos tecnológicos de la Corporación deberá acreditar el cumplimiento de lo dispuesto en el contrato mediante la supervisión y ejecución de todas las actividades del proyecto.
 - Toda actividad en función del proyecto deberá estar acorde a las metodologías, estándares y procedimientos definidos por la Corporación.

3.4.6. Control de cambio en desarrollo.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 25 de 59

- Le compete al área de desarrollo: elaborar, difundir y supervisar la adecuada utilización del procedimiento de control de cambios o versionamiento del desarrollo de software.

3.4.7. Análisis de requerimiento.

- En todo proyecto se debe realizar un análisis previo donde se determine las necesidades que deben ser suplidas con el desarrollo.
- Al menos un representante del área o del grupo de usuarios de un sistema, deberá ser partícipe del levantamiento de información, toma de decisiones y gestión de requerimientos del desarrollo. Llevando una bitácora del proceso y evolución de este.
- Para todo desarrollo se deberá llevar un registro de la gestión realizada, que incluya un formato para el levantamiento de información con datos personales de(los) usuario(s) y, los aspectos más relevantes.
- Con el pliego de requisitos sea para creación o modificación de un sistema, el área de desarrollo dará a conocer una matriz con las ventajas y desventajas del desarrollo.
- Antes de dar inicio al desarrollo, se dejará consignado el documento de requerimiento con sus opciones de ejecución como el acordado a desarrollar.

3.4.8. Diseño lógico.

- Todo requerimiento aprobado se constituirá como proyecto y, cada proyecto deberá contar con diseño lógico y técnico.
- El diseño lógico debe contener:
 - Documentación completa y detallada que contenga los procedimientos, estándares y metodologías definidas e integre el diseño lógico.
 - Estructura modular del sistema definido y documentado. Que tenga posibilidad de integración con otros sistemas si así se requiere.
 - Definición de los componentes y programas nuevos o modificados.
 - Definición de la forma de interacción del nuevo sistema o el sistema modificado con los usuarios finales.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 26 de 59

- Instructivo o manual que permita dar más claridad al usuario durante su navegación por todo el sistema, esto incluye botones, íconos, combinación de teclas, funciones disponibles, opciones de menú, entre otros.
 - Descripción detallada de los campos e información producida como informes y reportes que genera el sistema.
 - Requisitos de seguridad, rendimiento, respaldo, recuperación y depuración de datos con los que cuenta el sistema.
 - Esquema de seguridad para la identificación y autenticación de usuarios.
 - Privilegios y controles de acceso.
- El diseño técnico debe contener:
 - Arquitectura física del sistema, coherente a las funcionalidades esperadas y medio tecnológico donde se desenvuelve.
 - Definición del medio tecnológico ajustado conforme a los lineamientos de la dependencia que lidere los procesos tecnológicos de la Corporación.
 - Definición de elementos que configuran el medio tecnológico como lo son: equipos de cómputo y de telecomunicaciones (computadores, servidores, periféricos, sistemas operativos, conexión de red, sistemas gestores de base de datos, firewall, librerías, protocolos de comunicación, entre otros.)
 - Consideraciones en capacidad y tiempos de respuesta, demanda en volumen y otros que se puedan determinar en los estándares.

3.4.9. Construcción y desarrollo de software.

- El área de desarrollo garantizará el entorno para el desarrollo, pruebas y configuración del sistema, antes de iniciar con la ejecución del proyecto.
- La preparación deberá contemplar:
 - Constitución y puesta en funcionamiento de bases de datos, archivos y demás, pertinentes a la etapa de diseño.
 - Adecuación de datos e información de prueba para salvaguardar la integridad, confidencialidad y disponibilidad de los datos e información de producción.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 27 de 59

- Confirmación de los componentes, tanto lógico como físicos, en estado disponibles y accesibles para el desarrollo.
- Apego a los estándares y procedimientos previamente definidos.
- Registro, documentación y prueba de los elementos indentificados en el diseño del sistema.

3.4.10. Gestión de la calidad.

- Todo proyecto deberá ser aceptado previa validación y comprobación de que se ajusta al requerimiento inicial. Para ello se deberá suplir un proceso de aceptación del desarrollo.
- El proceso de aceptación incluirá los conceptos favorables a todas las etapas del desarrollo por parte del área de desarrollo, de quien hizo el requerimiento y la dependencia que lidere los procesos tecnológicos de la Corporación.
- El proceso deberá contener:
 - Validación funcional de una parte del sistema (pruebas unitarias) mediante prueba aislada y unitaria por parte del personal desarrollador.
 - Validación funcional de todo el sistema (pruebas integrales) mediante pruebas realizadas por el área de desarrollo donde integre todos sus elementos.
 - Validación funcional en ambiente controlado de prueba para los usuarios que harán uso del sistema.
 - Visto bueno de la dependencia que lidere los procesos tecnológicos de la Corporación donde confirme el cumplimiento de los estándares en disposición al ciclo de vida del desarrollo.

3.4.11. Implementación.

- La dependencia que lidere los procesos tecnológicos de la Corporación en conjunto con el área de desarrollo y la dependencia que hizo el requerimiento, efecturan un proceso de implementación del proyecto, situación que se debió considerar desde la etapa de análisis del requerimiento y en concordancia la acción para: instalación, configuración, modificación que será liberada al ambiente de producción o cualquiera que haya sido el objeto del proyecto.
- Requisitos para la implementación:

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 28 de 59

- El desarrollo debe ser aprobado y aceptado formalmente por quien hizo el requerimiento, antes de ser liberado a producción.
 - Siempre y cuando sea necesario, se deberá ejercer pruebas adicionales resultado de la fase de pruebas.
 - Una vez se acepte y pruebe el desarrollo, podrá insertarse en el entorno donde se ejecutará y, su estado quedará en revisión, seguimiento y mantenimiento. Para lo cual se dejará un acta.
 - En todo caso se debe realizar respaldo de datos.
 - Si se cuenta con dos sistemas (nuevo, anterior), de ser posible, se deberá implemetar el nuevo paulatinamente hasta que se acople a la funcionalidad del anterior, para luego este ser retirado.
- La dependencia que lidere los procesos tecnológicos de la Corporación deberá garantizar, o coordinar con el área usuaria, el proceso de capacitación y soporte de los nuevos desarrollos entregados.
 - La dependencia que lidere los procesos tecnológicos de la Corporación establecerá el procedimiento para el reporte, atención y seguimiento de los incidentes y novedades presentados con el desarrollo.
 - Le corresponde a la dependencia que lidere los procesos tecnológicos de la Corporación dar a conocer y supervisar el cumplimiento de las políticas, procedimientos y demás disposiciones para el desarrollo de software.

3.5. Adquisición, desarrollo y mantenimiento de sistemas de información.

Garantizar que la seguridad es parte integral de los sistemas de información, evitar errores, pérdidas, modificaciones no autorizadas o mal uso de la información en las aplicaciones, proteger la confidencialidad, autenticidad o integridad de la información con la ayuda de técnicas criptográficas, garantizar la seguridad de los sistemas de ficheros o carpetas, mantener la seguridad del software del sistema de aplicaciones y la información, y reducir los riesgos originados por la explotación de vulnerabilidades y/o errores técnicos publicados.

3.5.1. Requisitos de seguridad de los sistemas de información.

- La dependencia que lidere los procesos tecnológicos de la Corporación identificará y expondrá previo al desarrollo y/o implementación de sistemas de información, los requisitos de Seguridad.
- La dependencia que lidere los procesos tecnológicos de la Corporación es responsable por la implementación de los requisitos de seguridad identificados y consensuados.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 29 de 59

- Antes de la puesta en producción la dependencia que lidere los procesos tecnológicos de la Corporación someterá al sistema de información a las distintas pruebas de capacidad y seguridad.
- La dependencia que lidere los procesos tecnológicos de la Corporación deberá definir las distintas políticas de respaldo y continuidad de los sistemas de información.

3.5.2. Seguridad de las aplicaciones del sistema.

- La dependencia que lidere los procesos tecnológicos de la Corporación identificará y/o propondrá controles apropiados de validación de los datos de entrada, el tratamiento interno y los datos de salida.
- La dependencia que lidere los procesos tecnológicos de la Corporación desarrollará y/o usará herramientas de prueba idóneas que le permitan adelantarse a errores habituales como desbordamientos de memoria, llenado de tablas, consultas cíclicas e interminables.

3.5.3. Controles criptográficos.

- La dependencia que lidere los procesos tecnológicos de la Corporación identificará y/o propondrá controles criptográficos que permitan la protección de información sensible en los sistemas de información de Corantioquia (Por ejemplo: Tablas cifradas, uso del directorio activo como método de autenticación y autorización de usuarios, múltiples factores de autenticación, entre otros).

3.5.4. Seguridad de los ficheros o carpetas del sistema.

- La dependencia que lidere los procesos tecnológicos de la Corporación identificará y/o propondrá controles que permitan la protección de información contenida en las distintas carpetas del sistema de información, carpetas en el sistema operativo, ficheros en rutas no convencionales propias del aplicativo, entre otros.
- La dependencia que lidere los procesos tecnológicos de la Corporación evitará exponer datos sensibles en ambientes de prueba.
- La dependencia que lidere los procesos tecnológicos de la Corporación garantizará el adecuado almacenamiento de los códigos fuentes, además que deberán tener acceso restringido.

3.5.5. Seguridad en los procesos de desarrollo y soporte.

- La dependencia que lidere los procesos tecnológicos de la Corporación identificará e implementará un adecuado proceso de cambio,

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 30 de 59

actualización y soporte, en los que se incluyan tópicos como la documentación, el entrenamiento y preparación procedimental para usuarios, personal de soporte y administradores de los aplicativos.

3.5.6. Gestión de las vulnerabilidades y/o errores técnicos.

- La dependencia que lidere los procesos tecnológicos de la Corporación identificará, recomendará e implementará la adecuada gestión de errores o vulnerabilidades, que le permita tomar medidas sistemáticas y cíclicas para mantener la aplicación o aplicaciones en un adecuado nivel de actualización tanto en parches, como en versiones del sistema.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 31 de 59

4. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

ALCANCE

Establecer reglas y directrices para el uso controlado de los activos de información de Corantioquia, evitando accesos no autorizados, pérdida de información valiosa, divulgación no controlada, duplicación, adulteración, detención deliberada o extravío de algún activo de información.

LINEAMIENTOS:

4.1. Organización de la seguridad de la información.

Establecer las políticas que le permitirán a Corantioquia realizar la asignación de responsabilidades y gobernabilidad del Modelo de Seguridad y Privacidad de la Información (MSPI).

4.1.1. Estructura para la seguridad de la información.

- Se debe establecer un responsable del liderazgo y coordinación del MSPI, y velar porque las directrices estratégicas de seguridad de la información se cumplan en la Entidad. Este rol se denominará Líder del Modelo de Seguridad y Privacidad de la Información (MSPI).
- Se debe establecer una estructura de roles y responsabilidades asociadas a la salvaguarda de la seguridad de la información al interior de la Corporación.
- Se debe conformar un Comité de Seguridad de la Información que respalde y apoye las iniciativas de seguridad. Los miembros deben tener cierta relevancia en su cargo dentro de la organización y deben avalar y definir las directrices estratégicas de seguridad de la información. Este comité deberá reunirse por lo menos una vez por semestre. Las funciones de este comité son:
 - Revisión y aprobación de la política de seguridad y documentos asociados.
 - Seguimiento a incidentes de seguridad de la información.
 - Establecer planes de gestión de riesgos y análisis de resultados.
 - Definir planes de concientización.
 - Asegurar la implementación, mantenimiento y mejora continua del MSPI.
- Todos los funcionarios deben ser responsables del manejo adecuado de la información dentro y fuera de la Entidad, de su comunicación y divulgación, deben conocer la política general y las políticas específicas de la seguridad de la información y estar en la obligación de cumplirlas.
- En cada sesión del Comité de Seguridad de la Información se deberán realizar auditorías o revisiones al proceso de gestión de la seguridad de la información, es responsabilidad de todos los usuarios involucrados en

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 32 de 59

las auditorías, la atención y colaboración para la ejecución de las mismas.

- Es de vital importancia que la Entidad establezca contactos con grupos especializados en seguridad de la información. El líder seguridad de la información o el que él determine, deberá estar inscrito en foros académicos de seguridad de la información para mantenerse al día sobre amenazas y vulnerabilidades que puedan afectar a la Entidad.

4.1.2. Contratistas, proveedores y/o terceros.

- Se deben definir procedimientos para la autorización de acceso de contratistas, proveedores y/o terceros a los sistemas de información o servicios. Cada contratista, proveedor y/o tercero debe tener un responsable dentro de la Entidad que asegure que conozca la política general y las políticas específicas de la seguridad de la información y cumpla con las directrices descritas en esta.
- En los contratos con proveedores y/o terceros, Corantioquia deberá incluir una cláusula y un acuerdo de confidencialidad y no divulgación, que determinen las responsabilidades de las partes en cuanto al manejo de la seguridad de la información así como las consecuencias y medidas a tomar por el incumplimiento de las mismas.
- Se deben identificar los riesgos que implica el acceso de contratistas, proveedores y/o terceros a la Entidad e implementar controles que reduzcan dicho riesgo. Todo acceso de un contratista, proveedor y/o tercero a los sistemas de información de la Entidad debe ser autorizado y seguir los procedimientos establecidos.
- En los acuerdos con terceras partes que impliquen cualquier tipo de interacción con información de Corantioquia se deben incluir todos los aspectos de seguridad relevantes y el compromiso a su cumplimiento.

4.2. Controles de Acceso.

Definir el control de acceso a la información soportada por la infraestructura tecnológica y de telecomunicaciones de Corantioquia.

4.2.1. Directrices generales de control de acceso.

- El acceso a la información y los sistemas asociados deben estar debidamente controlados, asegurando que sólo el personal autorizado pueda tener acceso a la información, previa autorización formal por parte del dueño de la información.
- Se deberán mantener registros de las autorizaciones concedidas. Estas autorizaciones deben partir del principio de necesidad de saber, donde el usuario recibirá permisos solo para las actividades para las que fue contratado.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 33 de 59

- Los accesos concedidos deben contar con una revisión periódica para verificar si realmente siguen siendo necesarios o necesitan modificación.
- Cualquier cambio de cargo o área que realice un funcionario debe incluir una revisión de los permisos a los que tiene acceso buscando revocar aquellos que no son necesarios en las nuevas funciones que va a realizar.
- Se deberán establecer mecanismos de control para los casos en que por funcionalidades requeridas sea necesario compartir información. Estos mecanismos pueden ser:
 - Existencia de Autorización por parte del dueño de la información.
 - Soporte de un método de autenticación.
 - Exclusión de la información sensible.
- Se debe poder identificar el estado de los usuarios que están compartiendo la información y mantener un inventario de estos accesos.
- Se deberá mantener documentado el inventario de usuarios de los sistemas de información y los accesos y roles que se tienen en los diferentes sistemas de información y demás infraestructura tecnológica. Estos temas incluyen a los administradores de plataforma.
- Se deberán actualizar los accesos definidos debido a novedades a nivel del personal.
- Todo contratista, proveedor y/o tercero deberá tener acceso limitado a la información. No deberá tener alcance a ninguna información confidencial a no ser que sea autorizado explícitamente por el dueño de la misma, en cuyo caso se deberá firmar un acuerdo de confidencialidad y de no divulgación.
- Las cuentas asignadas a contratistas, proveedores y/o terceros deben tener un periodo de tiempo de vigencia o expiración asignado, que corresponde como máximo al tiempo de vigencia de contrato o alianza.
- La solicitud de acceso a los recursos informáticos brindados por Corantioquia solo será autorizado a personas que mantienen un vínculo con la Entidad. La incorporación de personas diferentes deberá ser autorizada por el responsable del contrato (en el caso de contratistas) o por el área que requiera que esta persona tenga acceso. (Estos accesos deberán responder el principio del mínimo privilegio).
- Las solicitudes de acceso deben contar, como mínimo, con la siguiente información:
 - Recursos y Servicios a los que requiere acceso.
 - Tiempo de acceso a esos recursos y servicios.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 34 de 59

- Compromiso de notificación frente al cese de actividades. (Novedades).
- El acceso a los componentes de la infraestructura tecnológica y de telecomunicaciones debe ser estrictamente controlado para prevenir el acceso no autorizado.
- Las cuentas de usuarios creadas deben ser únicas, personales e intransferibles, toda la responsabilidad de lo que suceda con esta cuenta recae sobre el titular de la cuenta.
- Se debe asegurar que el acceso a los servicios de red, datos y programas estén disponibles solamente para el personal específicamente designado por Corantioquia.
- Los responsables del ambiente tecnológico serán los únicos responsables de la ejecución de comandos especiales sobre componentes críticos, sea por medio de acceso local o remotamente.
- Antes de efectuar una solicitud, el usuario deberá identificar qué servicios requiere de los componentes de infraestructura tecnológica y de telecomunicaciones.
- Para cada servicio o aplicación, se debe seguir el procedimiento propio de control de acceso. En caso que este no exista deberá ser documentado y autorizado por el personal definido.
- Una vez se notifiquen modificaciones en el personal, se deberá evaluar si los accesos a los sistemas de información y componentes de la infraestructura tecnológica y de telecomunicaciones del usuario que se retira deben ser eliminados.
- En el caso de un cambio a los componentes de la infraestructura tecnológica y de telecomunicaciones el esquema de seguridad debe reevaluarse en su totalidad.
- Todo componente de la infraestructura tecnológica y de telecomunicaciones deberá tener un mecanismo que permita el registro de los usuarios de servicios informáticos y los derechos de acceso.
- Las acciones de acceso (login) a los sistemas de información, deberán dejar un registro de dicha acción para su observación y análisis.
- Los usuarios que se retiran de sus puestos de trabajo deben primero bloquear el acceso a su estación de trabajo o cerrar la sesión (logoff).
- La autorización para acceder a los componentes de la infraestructura tecnológica y de telecomunicaciones debe ser autorizado por el dueño del ambiente tecnológico.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88

Correo electrónico: corantioquia@corantioquia.gov.co

 CORANTIOQUIA	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 35 de 59

4.2.2. Directrices específicas de control de acceso a la información.

• Usuarios Privilegiados.

- Se considerará usuario privilegiado a aquellos que realizan actividades de administración en la infraestructura tecnológica y de telecomunicaciones con los máximos privilegios que requiere su función. Los usuarios privilegiados son todos aquellos identificadores de usuario que requieren ser asignados a funcionarios cuyo cargo y/o funciones está relacionado con la administración funcional y/o tecnológica de sistemas de información.
- Todo usuario con privilegio de superusuario o administrador del sistema, será creado particularmente. La asignación se deberá realizar al momento de la instalación de los componentes de la infraestructura tecnológica y de telecomunicaciones.
- Los usuarios privilegiados solo serán otorgados a aquellas personas que lo requieran para el cumplimiento de sus funciones.
- Deberá existir una cuenta de usuario que será utilizada exclusivamente para monitoreo por parte del área de seguridad de la información o quien haga sus veces, para revisar el uso de estos usuarios privilegiados.
- Las personas que por sus funciones requieran acceso de usuario privilegiado o niveles de permisos adicionales, deben solicitarlo siguiendo el procedimiento establecido por Corantioquia para solicitud de acceso a componentes de la infraestructura tecnológica y de telecomunicaciones.
- Ningún usuario privilegiado debe modificar información sin previa autorización de su dueño.
- Las cuentas de usuarios privilegiados y superusuarios deben ser de uso personal e intransferible.
- Las cuentas privilegiadas deben contar con una clave que debe ser almacenada en un lugar seguro y con acceso solamente a personal autorizado.

• Usuarios Genéricos.

- Cualquier área de Corantioquia, por medio de un responsable, podrá solicitar la creación de usuarios genéricos en los diferentes componentes de la plataforma tecnológica justificando por escrito la necesidad de los mismos y asumiendo

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 36 de 59

el conocimiento de las implicaciones de control que requiere la utilización de estos usuarios genéricos.

- La creación de un usuario genérico debe ser autorizada por el dueño de la Información, el Jefe inmediato y el área de Seguridad de la Información o quien haga sus veces.
- Los usuarios genéricos solo deben establecerse con fines de consulta de datos, no de actualización (ingreso, eliminación y modificación).
- Todas las cuentas con permisos de ingreso, eliminación o modificación de información deben ser de carácter personal y sus contraseñas deben seguir los parámetros establecidos por la Entidad.

• Usuarios con altos privilegios en Bases de Datos (Superusuarios).

- Los superusuarios de aplicativos que requieren acceso a las bases de datos son responsabilidad de los administradores de las bases de datos, quienes deberán monitorearlos.
- Al realizar la creación de cuentas, el administrador debe asegurarse que las transacciones que se realizan puedan ser asociadas con el sistema de información y el usuario que la realizó, para que de esta manera se puedan realizar seguimientos y auditorías.
- La creación de los superusuarios a nivel de bases de datos deberá ser definida y justificada técnicamente por los desarrolladores de los aplicativos y administradores de servicios informáticos.
- Debe evitarse la asignación de roles exclusivos del administrador de la base de datos a los usuarios que no requieran de dichas funciones.

• Actualización de accesos a componentes Tecnológicos.

- Debe existir un procedimiento formal para la creación, actualización y eliminación de accesos a los diferentes componentes de la plataforma tecnológica existentes en Corantioquia.
- Los dueños de la información, serán los responsables de velar por que los roles y/o perfiles de acceso existentes sean acordes con las funciones realizadas por cada uno de los usuarios.
- El acceso a componentes tecnológicos por medios remotos para actividades de mantenimiento, soporte y monitoreo por

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 37 de 59

parte del proveedor del componente, está permitido si la conexión remota cumple con los requerimientos de seguridad de Corantioquia, como acceso con protocolos seguros a través de VPN (Virtual Private Network).

4.2.3. No repudio.

Se debe contar con la capacidad de no repudio con el fin de que los usuarios eviten haber realizado alguna acción, incluyendo:

- Realizar trazabilidad de acciones para seguimiento de creación, origen, recepción, entrega de información, entre otros.
- Se deberá retener la información de acciones realizadas por usuarios (logs) por un periodo de tiempo definido por la Corporación, de acuerdo con su necesidad actual.
- El plan de auditoría debe incluir la revisión de acciones críticas de las partes interesadas.
- En los intercambios electrónicos de información se garantizará el no repudio.

4.2.4. Integridad.

Entendiendo la información como uno de los activos más importantes de la Corporación, deberá darsele un manejo íntegro a toda la información interna y externa, tanto por parte de los funcionarios como de los contratistas y externos. Así, toda la información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas correspondientes y a través de los medios correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información.

Para los funcionarios de la Corporación con vinculación contractual, se recomienda incluir el compromiso del manejo íntegro e integral de la información en las cláusulas del respectivo contrato, bajo la denominación de Cláusula de integridad de la información.

Esta política aplica al personal vinculado a la Corporación a lo largo de la vigencia de su contrato o periodo de la vinculación.

4.3. Acceso físico a la dependencia que lidere los procesos tecnológicos de la Corporación.

- El acceso a los entornos físico de la dependencia que lidere los procesos tecnológicos de la Corporación donde se desarrolle actividades que manejen temas confidenciales y, donde haya equipos de cómputo y equipos de telecomunicaciones de suma importancia para la operatividad de la entidad, será restringido. Su acceso deberá ser autorizado por el responsable del área, además que debe garantizar el cumplimiento de las disposiciones para la protección y conservación de los datos e información.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 38 de 59

- Cualquier persona que no pertenezca a la dependencia que lidere los procesos tecnológicos de la Corporación y que desea acceder a esta, deberá ser autorizado y acompañado permanentemente por personal del área. Si se necesita un servicio o radicar un requerimiento, el solicitante deberá hacer uso de los diferentes canales dispuestos para ello.

4.4. Seguridad de las comunicaciones y operaciones.

Asegurar la operación correcta y segura de los servicios de procesamiento de información mediante la definición de actividades orientadas a establecer controles de seguridad y la definición de estándares y lineamientos de seguridad para ser cumplidos por toda la organización.

4.4.1. Administración de comunicaciones y operaciones.

- Antes de que cualquier sistema operativo, herramienta y/o software en general sea instalado en la Entidad, el personal designado para tal fin debe deshabilitar o renombrar todas las cuentas privilegiadas existentes por defecto o creadas por los proveedores. En caso de existir cuentas privilegiadas que no se puedan deshabilitar o renombrar, se deberá cambiar las claves que traen por defecto.
- Todos los sistemas de información deberán tener la hora sincronizada.
- Las configuraciones, protocolos o software que no sean utilizados, y que no sean necesarios para las labores diarias, deberán ser desinstalados o deshabilitados.
- Las extensiones, modificaciones o reemplazos a los sistemas operativos de producción deben ejecutarse antes bajo ambientes controlados de desarrollo y pruebas, y deben tener aprobación del Comité de cambios.
- El área de Seguridad de la Información o quien haga sus veces, debe realizar revisiones periódicas o evaluaciones de vulnerabilidades sobre los sistemas operativos de producción.
- Todos los sistemas operativos en producción, los sistemas de administración de bases de datos, Firewalls, IDS (sistema de detección de intrusos), IPS (sistema de prevención de intrusos), aplicaciones y todo el software existente en la plataforma de Corantioquia, debe mantenerse en las versiones estables más recientes que mantengan compatibilidad con los demás componentes de los sistemas de información.
- Bajo aprobación del Comité de Cambios, para todas las modificaciones en los sistemas de producción se deben desarrollar

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 39 de 59

procedimientos adecuados de devolución (Rollback), como también antes de cada cambio realizar un respaldo de seguridad, según lo indica el procedimiento de cambios, los cuales permitan devolverlos rápida y oportunamente a las condiciones previas al cambio más reciente en el software.

- La dependencia que lidere los procesos tecnológicos de la Corporación será responsable del monitoreo de la capacidad de la plataforma tecnológica procurando identificar oportunamente elementos que puedan conllevar a la no disponibilidad de la misma o la afectación de la información que soportan.
- Se debe realizar una revisión periódica de las reglas de los Firewalls, routers y switches de Core (mínimo cada 6 meses), de manera que siempre se tenga una configuración actualizada y adecuada. Se debe generar un informe del resultado de la revisión de reglas con la información de la reglas borradas o cambiadas.
- El manejo de equipos de seguridad solo debe ser realizado por el área de Seguridad de la Información o quien haga sus veces.
- Los equipos de la infraestructura de telecomunicaciones solo deben ser manejados por el personal designado por la dependencia que lidere los procesos tecnológicos de la Corporación.

4.4.2. Protección contra software malicioso.

- Se debe contar con un software antivirus verificado y aprobado por el área de Seguridad de la Información (o quien haga sus veces), que se encuentre monitoreando y proteja todas las estaciones de trabajo existentes en la plataforma informática de Corantioquia. Este debe mantenerse al día y tener políticas de actualización de firmas y software.
- Cualquier usuario que sospeche de una infección por un software malicioso debe apagar inmediatamente el computador involucrado, desconectarlo de cualquier red, contactar a la dependencia que lidere los procesos tecnológicos de la Corporación y evitar cualquier intento de eliminar el virus.
- Solamente los administradores de sistemas y/o personal autorizado por la dependencia que lidere los procesos tecnológicos de la Corporación y el área de Seguridad de la Información (o quien haga sus veces) deben realizar las tareas de desinfección de los elementos de la red informática de Corantioquia.
- Cualquier sistema de almacenamiento como CD-ROMs, cartuchos ópticos, cintas Digital Audio Tape (DAT) o cintas de audio digital, etc., provistos por entidades externas no deben ser utilizados en los sistemas de Corantioquia, a menos que éstos medios hayan sido analizados con

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 40 de 59

el sistema antivirus de la Entidad y se asegure que no contienen ningún software malicioso.

- Todos los servidores y computadores de Corantioquia, deben estar en constante análisis por el antivirus definido. Se debe programar una tarea de análisis periódico de los sistemas y evaluación de resultados por parte del área de Seguridad de la Información o quien haga sus veces.
- Los usuarios no deben escribir, generar, compilar, copiar, almacenar, propagar, ejecutar o intentar introducir cualquier código de aplicación diseñado para auto replicarse, deteriorar o que obstaculice el desempeño de cualquier sistema de Corantioquia o de cualquier entidad externa.
- No deben ejecutarse actualizaciones a los programas de software instalados en los computadores asignados por Corantioquia para el desarrollo de las labores contratadas, éstas actualizaciones serán realizadas o dirigidas directamente por la dependencia que lidere los procesos tecnológicos de la Corporación y el área de Seguridad de la Información o quien haga sus veces.

4.4.3. Protección durante la navegación.

- Se debe tener un sistema de control de navegación en Internet que proporcione análisis de sitios malicioso o con Malware y que permita implementar políticas de navegación basado en los grupos del directorio activo.
- Se debe restringir el acceso a sitios peligrosos, donde se pueda compartir información en línea (como son cualquier multiplataforma en la nube para alojamiento de archivos) o que puedan afectar la productividad del funcionario.
- Se deben generar reportes periódicos donde se observe los usuarios que más consumen ancho de banda, los sitios más visitados, etc., y con estos análisis tomar decisiones que mejoren el nivel de servicio de Internet.
- Se deben realizar campañas sobre el buen uso de Internet para concientizar a las personas sobre los peligros de descargar archivos, acceder a sitios desconocidos o de baja confianza y aceptar los mensajes sobre instalación de software que brinde el navegador y el acceso a sitios seguros.
- Se deberán establecer mecanismos de protección y autenticación para evitar que contratistas, proveedores y/o terceros no autorizados accedan a la infraestructura tecnológica interna de Corantioquia.
- Se debe configurar una red independiente de acceso a Internet para los invitados, la cual debe manejar un portal cautivo donde se puedan

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 41 de 59

autenticar. Estos accesos deben ser autorizados y se deben asignar por un tiempo definido.

- Ningún funcionario debe utilizar software obtenido desde Internet o de una persona u organización diferente a los distribuidores confiables o conocidos, a menos que el software haya sido examinado en busca de código malicioso y que haya sido aprobado por el área de Seguridad de la Información o quien haga sus veces.
- En ningún momento se debe almacenar información de la Entidad en servidores públicos en Internet.

4.4.4. Seguridad de medios.

- Se debe establecer los mecanismos de protección adecuados para los medios de almacenamiento (USB, CD-ROMs, Discos extraíbles, cintas, memorias, etc), entre los que se proponen: la implementación de un DLP (Data Lost Prevention), bloqueo de puertos, módulo para protección de información en la nube, con el fin de mitigar el riesgo de fuga de información.
- Cuando se requiera, por el desarrollo de las funciones, almacenar información en dispositivos móviles se deberá revisar la clasificación del activo de información a fin de verificar que esta pueda ser almacenada en este tipo de dispositivos y se debe solicitar autorización al área de Seguridad de la Información o a quien haga sus veces y al Jefe respectivo.
- Se debe establecer el tipo de protección que tendrán los medios que almacenan información de acuerdo a su clasificación, para evitar riesgos como divulgación, modificación, pérdida y destrucción de manera no autorizada.
- La protección y almacenamiento de la información debe ser definida y tratada de acuerdo a su nivel de clasificación en el inventario de activos.
- Se debe asegurar que todo dispositivo de almacenamiento (memorias, cintas, etc.), y la información que este guarda, debe conservar las características iniciales con el paso del tiempo. (Evitar la pérdida de información por desactualización de las tecnologías que soportan ese tema).
- Se deben definir, de acuerdo a la sensibilidad de la información y su clasificación, los niveles de autorización y acceso para su manipulación y manejo en los medios de almacenamiento donde se encuentre soportada.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 42 de 59

- Se deberán realizar respaldos periódicos del software y la información importante en los sistemas de información de la Entidad. Estos respaldos se deben realizar con la frecuencia apropiada para cada sistema de información. Se debe validar que las copias sean correctas y realizar pruebas de funcionamiento periódicas.
- Las copias de seguridad generadas en el Centro de Cómputo, deben residir en un centro de almacenamiento fuera del edificio donde este se ubique, manteniendo las condiciones requeridas para el almacenamiento. Se deberán mantener los controles y procedimientos necesarios para conocer el estado de cada copia de seguridad.
- Los periodos de retención de copias de seguridad deberán satisfacer los requerimientos de aseguramiento de la continuidad de sus funciones.
- Se deberán realizar pruebas periódicas para asegurar que los equipos y los medios de almacenamiento no se deterioren para asegurar que cumplan con su función cuando se necesiten.
- Se deberá establecer un procedimiento para la eliminación de archivos y medios obsoletos con estándares de borrado seguro definidos por el área de Seguridad de la Información o quien haga sus veces.
- Se deberán implementar procedimientos para preparar, almacenar y probar periódicamente la integridad de las copias de seguridad y de toda la información necesaria para restaurar el sistema a una operación normal.
- Se deberán mantener copias de seguridad de todas las versiones de software, parámetros y configuraciones requeridas para una correcta restauración de la información contenida en los medios de almacenamiento.
- Se debe mantener un control de contenido de los medios utilizados, donde se registre información que permita la identificación correcta de la información allí contenida por ejemplo: fechas, información, expiración, lugar de almacenamiento, etc.
- El dimensionamiento de los requerimientos para el manejo de la estrategia de copias de respaldo de la información, será definido por la dependencia que lidere los procesos tecnológicos de la Corporación.

4.4.5. Administración y controles de red.

- La dependencia que lidere los procesos tecnológicos de la Corporación debe asegurar que las configuraciones de todas las máquinas conectadas a la red de Corantioquia cumplan con la política general y las políticas específicas de seguridad de la información.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 43 de 59

- Los encargados de la arquitectura de la plataforma informática y los desarrolladores de los sistemas de información deben restringir el uso de interfaces de red externas y de protocolos a aquellos que hayan sido expresamente aprobados por el área de Seguridad de la Información. Y los accesos se deben restringir solo a quien los necesita.
- Cuando se haga control remoto para labores de soporte o mantenimiento por la dependencia que lidere los procesos tecnológicos de la Corporación, el usuario solicitante deberá estar frente a su computador monitorizando las actividades desarrolladas.
- El personal de la dependencia que lidere los procesos tecnológicos de la Corporación no está autorizado para acceder a la información que se encuentra almacenada en los equipos a los cuales acceden los usuarios funcionales, sin una justificación expresa de la Dirección o las Subdirecciones de la Corporación, respetando la Política de Tratamiento de Datos Personales.
- Notificar con antelación al usuario cuando se vayan a realizar labores sobre su equipo.
- Todos los computadores multiusuario conectados a Internet deben ser monitoreados con un sistema de detección de intrusos (IDS) aprobado por el área de Seguridad de la Información.
- Los servidores publicados a Internet deben ser ubicados en una zona desmilitarizada, protegida por un firewall.
- Todas las conexiones entre los computadores de Corantioquia e Internet deben pasar a través de un firewall aprobado y los controles de acceso relacionados.
- El establecimiento de una conexión directa entre los sistemas de Corantioquia y computadores de organizaciones externas, debe ser a través del firewall de la Entidad y debe ser aprobado por el área de Seguridad de la Información.
- El área de Seguridad de la Información o quien haga sus veces debe mantener un inventario actualizado de las todas las conexiones de Corantioquia con redes externas.
- En lo posible no se deben utilizar protocolos de autenticación inseguros (como telnet, FTP), se debe tratar de utilizar protocolos que transmitan las credenciales cifradas. En caso de solo poderse utilizar protocolos inseguros se deben implementar listas de control de acceso con las máquinas que necesitan acceder al sistema y estos deben ser justificados y documentados (asumiendo el riesgo) ante el área de Seguridad de la Información o quien haga sus veces.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 44 de 59

- Las redes inalámbricas que utilice Corantioquia, deben estar configuradas para utilizar cifrado fuerte en sus comunicaciones y autenticación contra el directorio activo.
- La dependencia que lidere los procesos tecnológicos de la Corporación debe establecer mecanismos de autorización para controlar quien puede realizar llamadas y bajo qué condiciones.
- La dependencia que lidere los procesos tecnológicos de la Corporación debe establecer controles de cifrado que permitan proteger la confidencialidad de las llamadas telefónicas.
- La dependencia que lidere los procesos tecnológicos de la Corporación deberá proteger los componentes que hacen parte del servicio de Telefonía IP para evitar ataques a la misma.
- Ningún funcionario incluyendo a los administradores de la plataforma podrá interceptar o escuchar las llamadas de otros funcionarios de Corantioquia, salvo por orden judicial.
- Sólo se podrán grabar las llamadas cuando esto esté expresamente autorizado por la Entidad o autoridad competente y haya sido informado al personal que está interactuando en la misma.

4.4.6. Documentación de la seguridad del sistema.

- Toda la documentación que describe los sistemas de información o los procedimientos de sistemas de Corantioquia, debe ser revisada y aprobada por los respectivos coordinadores antes de ser liberada a terceras partes.
- Toda la documentación empleada por Corantioquia para reglamentar el uso, operación y administración de los sistemas de información no debe ser conservada, extraída o compartida por los funcionarios de la Entidad.
- Toda la documentación empleada por Corantioquia para reglamentar el uso, operación y administración de los sistemas de información debe mantenerse disponible para su consulta por parte de los autorizados y de igual manera los responsables de la misma deben garantizar su actualización.

4.4.7. Intercambio de información y de software.

- Todos los servidores de Corantioquia que manejan datos de usuarios con organizaciones o personas externas, deben emplear certificados digitales y deben utilizar cifrado para transferir información entre los sistemas involucrados.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 45 de 59

- Toda información sensible como pagos, números de cuentas corrientes, de tarjetas de crédito, claves, entre otros, debe permanecer cifrada durante su transporte y almacenamiento.
- Cada buzón de correo electrónico debe tener un espacio controlado por la dependencia que lidere los procesos tecnológicos de la Corporación, según la política de uso definida.
- Los administradores de sistemas de Corantioquia, deben establecer y mantener procesos sistemáticos para limitar el uso y/o transferencia de archivos con extensiones potencialmente peligrosas, detección de contenido malicioso o spam.
- La Entidad, por sí misma, está autorizada a desactivar y posteriormente cancelar las cuentas de correo electrónico que no presenten uso en 2 meses, a menos que el dueño del buzón se encuentre en vacaciones, licencia o incapacidad.

4.4.8. Protección y respaldo de la información.

- Para Corantioquia la información es considerada como un activo de valor estratégico, por esta razón se deberán implementar los mecanismos necesarios que garanticen un adecuado tratamiento en el ciclo de vida de la información, especialmente para los casos que requieren mantener la disponibilidad de la misma.
- Se deberá preservar la seguridad de la información dando cumplimiento a los principios de Confidencialidad, Integridad, Disponibilidad de Corantioquia, según el nivel de importancia de la misma.
- Los usuarios de Corantioquia, dueños de la información, son responsables de alojar la información que necesita ser respaldada en los servidores de archivo de la Corporación o la cuenta de OneDrive de cada usuario.
- Se debe realizar seguimiento periódico semestral a los respaldos de información que se realiza de cada funcionario según su nivel de clasificación. En caso de detectar incumplimiento del lineamiento anterior, por primera vez se enviará un correo por parte de la dependencia que lidere los procesos tecnológicos de la Corporación, de persistir el incumplimiento se enviará un correo por parte del Subdirector Administrativo y Financiero y por tercera vez se notificará por parte de la Dirección General.
- Se deben aplicar los controles para la protección de la información según su nivel de clasificación. Así mismo deberán alertar al dueño de la información cuando un activo digital de información requiera medidas especiales de protección.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

 CORANTIOQUIA	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 46 de 59

- Se debe realizar una revisión periódica semestral de los correos corporativos por cada usuario, para posteriormente realizarles un respaldo de la información con el fin de liberar espacio de almacenamiento. Para el caso de la liberación de licencia de Office 365, se realizará un backup de la información del correo del usuario en un archivo .pst como de la información alojada en OneDrive, para luego proceder a la liberación de la cuenta en la plataforma de Office 365, este proceso se realizará una vez se retire el usuario de la Corporación.

4.4.9. Registro histórico de actividades, información incluida en los logs.

- Todas las aplicaciones de producción que manejen información sensible de Corantioquia, deben generar logs que muestren cada modificación, incorporación y borrado de la información. Esto incluye modificaciones a los sistemas de producción y modificaciones a los sistemas fuente.
- Los sistemas que manejen información valiosa, sensible o crítica deben además contener y activar forzosamente el log sobre todos los eventos o procesos relacionados con la seguridad de acceso a los mismos. Ejemplo: Varios intentos de contraseña, intentos de uso de privilegios no autorizados, entre otros.
- Los logs de procesos relevantes deben de proveer información suficiente para soportar auditorías y contribuir a la eficiencia y cumplimiento de medidas de seguridad. Es importante que la dependencia que lidere los procesos tecnológicos de la Corporación acuerde con el dueño de la información sobre cualquier característica especial que estos logs deban incluir, de acuerdo a requerimientos internos o con autoridades externas.
- El acceso a los sistemas debe ser a través de usuarios personales y únicos. En el caso de usar usuarios de servicio o genéricos, se les debe asignar un responsable. Esto para hacer más fácil el registro de actividades.
- Se deben definir períodos para la depuración de logs, dependiendo de la plataforma, su capacidad, las necesidades de sus funciones y de las normas o regulaciones que puedan aplicar. Durante este período, el administrador del sistema y/o dueño de la información, se debe asegurar que éste no sea modificado, cerciorarse de que no sea leído por personal no autorizado y de igual manera garantizar su retención por el periodo necesario para sus funciones o que obligue la ley. Estos aspectos son importantes para la corrección de errores, auditorías o revisión de brechas de seguridad.
- Las principales aplicaciones, plataformas de producción, bases de datos, equipos de red y cualquier otro elemento que contenga, maneja o procese información de usuarios o de sus funciones deben tener

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 47 de 59

registro de logs activo de manera que permita identificar y detectar eventos o incidentes en la infraestructura de la Entidad.

- Todos los sistemas de Corantioquia, incluyendo los computadores y servidores, deben tener el horario y calendario sincronizado a un servidor central, el cual se debe sincronizar de una entidad externa. Esto para facilitar actividades de rastreo mediante los logs de los sistema.
- Los mecanismos para detectar y registrar eventos de seguridad significativos, deben ser resistentes a los ataques. Estos ataques incluyen intentos de desactivación, modificación, o borrado del software de log. Esto incluye tomar las medidas necesarias para que, aún cuando el log sea apagado o modificado, esta suspensión o modificación quede registrada en el mismo. Además, todos los sistemas de información de la corporación deben contar con dichos mecanismos.
- Los logs de todos los sistemas y aplicaciones deben ser conservados de forma tal, que no puedan ser revisados o visualizados por personas no autorizadas. Los servidores públicos, contratistas, proveedores y/o terceros autorizados deben contar con una autorización la dependencia que lidere los procesos tecnológicos de la Corporación.
- El Comité de Seguridad de la Información debe solicitar un adecuado manejo de los archivos log de los sistemas que los servidores públicos, contratistas, proveedores y/o terceros la dependencia que lidere los procesos tecnológicos de la Corporación manejan.

4.5. Gestión de incidentes de seguridad de la información.

Asegurar que los eventos y debilidades de seguridad de la información asociados con los sistemas de información se comunican de una manera que permita que se tomen acciones correctivas oportunas y responder a los incidentes en tiempo y forma apropiada para recuperar la actividad de la Entidad, considerando los aspectos legales aplicables.

4.5.1. Gestión de los incidentes y las mejoras en la seguridad de la información.

- La Entidad debe establecer un procedimiento formal para el reporte de eventos de Seguridad de la Información que contenga la situación presentada y de inmediato se notificará al Líder de Seguridad para su valoración, gestión y toma de acciones respectivas. Este procedimiento debe contar con los niveles de escalamiento pertinentes.
- Todos los servidores públicos, contratistas, proveedores y/o terceros de la Entidad deben tener conciencia sobre los procedimientos de reporte de los diferentes tipos de eventos y las debilidades que puedan tener impacto en la seguridad de los activos de información de los que hacen uso. Se debe contar con un punto único de contacto y cada funcionario debe cumplir con el reporte de los eventos tan pronto le sea

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

 CORANTIOQUIA	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 48 de 59

posible. La dependencia que lidere los procesos tecnológicos de la Corporación debe saber clasificar el incidente como de seguridad y seguir el respectivo procedimiento.

- La Entidad debe incluir en la inducción o sensibilización sobre seguridad de la información, temas sobre cómo identificar y reportar incidentes de seguridad y su responsabilidad respecto a estos temas.
- La Entidad debe establecer un procedimiento formal sobre como recolectar y asegurar los rastros y la evidencia para auditoría y los demás entes de control que así lo requieran.
- Se debe elaborar un procedimiento de tratamiento de incidentes de seguridad, su documentación y el almacenamiento de evidencias de manera segura.
- Los procedimientos respecto a incidentes de seguridad de la información deben manejarse por el área de Seguridad de la Información o quien haga sus veces.

4.6. Gestión de la continuidad tecnológica.

Reaccionar a la interrupción de los sistemas críticos de la Entidad procurando su funcionamiento ante la ocurrencia de un evento que afecte la continuidad de los servicios tecnológicos que soportan la operación.

4.6.1. Aspectos de la gestión de continuidad tecnológica.

- La Entidad deberá realizar todas las definiciones del proceso de gestión de la continuidad de sus funciones, su marco de gobierno y los lineamientos tendientes a reducir al mínimo la materialización de un riesgo de no continuidad en los procesos críticos.
- La base para el desarrollo del proceso de gestión de la continuidad tecnológica ante la ocurrencia de un desastre (DRP), es el análisis de impacto al negocio BIA (Business Impact Analysis). En este análisis se debe definir el nivel de criticidad de los diferentes procesos y aplicaciones que los soportan, considerando la cantidad de información que el proceso puede perder (RPO) y el tiempo que tardaría nuevamente en estar operativo (RTO) el proceso o aplicación luego de la ocurrencia de un desastre. Estos acuerdos de niveles de servicio (RPO y RTO) deberán ser definidos por la Corporación de acuerdo con la criticidad de cada uno de los sistemas de información, las necesidades de los procesos de la Corporación, y deberá alinearse con el catálogo de servicios del área de Tecnología.
- Se deben tener documentados y en constante actualización los planes de recuperación (movilización y retorno) de las aplicaciones críticas de la Entidad. Adicionalmente se debe cumplir con el calendario anual de

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 49 de 59

pruebas, incluyendo como mínimo una prueba unitaria (prueba en un ambiente controlado no productivo) y una prueba de operación real en el ambiente de DRP.

- Se debe familiarizar a los funcionarios que tienen roles o funciones dentro del DRP, en las características del proceso y las responsabilidades de su rol.
- Se debe velar por la gestión de interrupciones para salvaguardar la disponibilidad de los servicios.

4.6.2. Gestión de cambios.

Los cambios deben ser clasificados para darles la gestión adecuada para sus pasos a producción, buscando realizarlos bajo condiciones controladas que afecten mínimamente la disponibilidad de los sistemas y servicios.

- Soporte a la gestión de cambios: Se debe definir plantillas y orientar a los usuarios en el proceso de autorización de cambios, facilitando el entendimiento del proceso.
- Registro y pre-evaluación de Solicitudes de cambio: Se deben descartar las solicitudes de cambio que no cuenten con la información requerida o que no sean viables.
- Clasificación y evaluación de Solicitudes de cambio: Se debe verificar la prioridad del cambio solicitado y determinar las autorizaciones necesarias para aprobarlo
- Programación de cambios: Se debe acordar la programación preliminar para la implementación del cambio, asignando las responsabilidades necesarias y respetando la disponibilidad de los sistemas y servicios
- Evaluación de cambios: Evaluar la implementación del cambio y los resultados obtenidos, de manera que se conserve un historial completo de actividades para referencias futuras.

4.6.3. Segregación de ambientes.

En busca de minimizar los riesgos de puesta en funcionamiento de cambios y nuevos desarrollos, y de minimizar el impacto de la indisponibilidad del servicio durante las fases de desarrollo, pruebas y producción, se recomienda conservar al menos tres ambientes en el proceso de desarrollo y despliegue de cambios (Desarrollo, Pruebas y Producción). Cada ambiente debe tener su propia base de datos y su copia de la aplicación, de manera que no haya interferencia entre los ambientes y entre los participantes del proceso.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 50 de 59

5. POLÍTICAS SOBRE ACTIVOS DE INFORMACIÓN

ALCANCE

Regular la ocupación apropiada de los activos de información, suministrados a los funcionario y terceros autorizados para el cumplimiento de sus funciones. Donde cada activo deberá aprovecharse con ética y en cumplimiento de las leyes y reglamento vigente, evitando pérdidas o daños sobre cometido la gestión e imagen de la Corporación.

LINEAMIENTOS:

5.1. Gestión de Activos.

Definir la protección adecuada de los activos de información de la Entidad, definiendo el debido control sobre la información, incluyendo el inventario de todos los activos, su clasificación, propietarios y las directrices de tratamiento.

5.1.1. Responsabilidad sobre los activos.

- Todos los procesos incluidos en el alcance del Modelo de Seguridad y Privacidad de la Información Modelo de Seguridad y Privacidad de la Información deben realizar el inventario de activos de información de su proceso, basados en el instructivo de inventario y valoración de activos de información definido por la Entidad. Todos los activos deberán estar debidamente identificados y clasificados. Además deben asignar un propietario para cada activo y definir las regulaciones para el uso adecuado de dicha información.
- El líder de seguridad de la información deberá validar que todos los procesos estén desarrollando las actividades de inventario y valoración de activos de información.
- La Oficina de Control Interno es responsable de realizar auditorías para verificar que los procesos mantienen actualizado su inventario de activos de información y que cumplen con el instructivo definido para tal fin.
- Los usuarios de la información son responsables, mientras tengan la información bajo su control o acceso, de mantener los niveles de protección y clasificación establecidos para la misma en todo momento, haciendo uso adecuado de los recursos a su disposición.

5.1.2. Propietarios de los activos de información.

- Los propietarios de los activos de información son los procesos que tengan responsabilidad directa designada de la Entidad sobre los mismos. Además, dichos propietarios de los activos deben definir la prioridad y protección para el acceso a estos.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 51 de 59

- Los propietarios de los activos de información, con la asesoría del líder del MSPI, son los que definirán los mecanismos de protección y los permisos de acceso a estos.
- Los propietarios de los activos de información son responsables de su valoración y encargados de garantizar que las personas que tengan acceso a estos, los traten de acuerdo a su valor para la organización.
- Los propietarios pueden entregar los activos de información para custodia a los procesos designados por la Entidad; sin embargo, la responsabilidad de su seguridad no se traslada a este último.

5.1.3. Clasificación y etiquetado.

- Los activos de información serán clasificados teniendo en cuenta la valoración de los mismos y el procedimiento definido para tal fin.
- Los activos de información deberán ser etiquetados para que sean tratados de acuerdo con su nivel de importancia para Corantioquia y atendiendo el instructivo correspondiente.
- Los niveles de clasificación y protección establecidos para los activos de información de Corantioquia deberán ser mantenidos en todo momento. Por lo tanto, la Entidad garantizará los recursos requeridos para su adecuada protección.

5.2. Respaldo y protección de datos e información.

5.2.1. Fundamentos de respaldo y protección de datos e información.

- La dependencia que lidere los procesos tecnológicos de la Corporación deberá de manera periódica y con el apoyo de todas la dependencias, analizar y determinar la información y datos que son clasificados con valoración de seguridad “Crítica” para su correcto respaldo de seguridad definido con una frecuencia de acción y, con el apoyo del inventario consolidado de activos de información.
- La dependencia que lidere los procesos tecnológicos de la Corporación establecerá y controlará la ejecución de respaldos de seguridad y protección de los datos. Creando un documento y esquema guía para su gestión.
- Cada usuario será responsable de la información que utiliza, gestiona y respalda en su equipo de cómputo. La dependencia que lidere los procesos tecnológicos de la Corporación será responsable de la información y datos contenidos en los servidores por medio de la unidades de red. Si algún usuario necesita ayuda para realizar copias de seguridad, podrá elevar el requerimiento a la dependencia que lidere los procesos tecnológicos de la Corporación para ese propósito.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88

Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 52 de 59

- Corantioquia dispone de los recursos en red como repositorios para realizar los respaldos de seguridad. Los usuarios deberán hacer uso de dichos recursos.
- La actualización periódica y configuraciones necesarias que blinden la efectividad y eficiencia de las copias de seguridad recae la dependencia que lidere los procesos tecnológicos de la Corporación y al administrador del centro de datos.
- Únicamente esta autorizado personal la dependencia que lidere los procesos tecnológicos de la Corporación y la administración del centro de datos para proceder con los respaldos de seguridad. El personal deberá ser idóneo en el manejo y gestión de herramientas, procedimientos y protocolos para lograr el propósito.
- Cuando se requiera cambio de equipo de cómputo, la dependencia que lidere los procesos tecnológicos de la Corporación hará las copias de seguridad necesarias para lograr que durante la migración se conserve la unicidad funcional del equipo.
- La dependencia que lidere los procesos tecnológicos de la Corporación garantizará la preservación de datos e información que haya contenido en los servidores de la entidad y que posean relación a las funciones de esta, según lo acordado con el dueño de la información sobre el tiempo de retención.
- De acuerdo a la tabla de retención documental (Gestión Documental), los datos e información será conservada por un período de tiempo, razón por la cual deberán informar la dependencia que lidere los procesos tecnológicos de la Corporación la disposición final de estos datos cumplido el plazo.
- La dependencia que lidere los procesos tecnológicos de la Corporación definirá perfiles, roles, funciones y responsabilidades de los usuarios con sus respectivos privilegios de acceso a los sitios donde se respalda la seguridad. De lo contrario, el acceso es restringido.
- Todos los datos e información transaccional de la Corporación deberá ser respaldada para garantizar su conservación.
- La dependencia que lidere los procesos tecnológicos de la Corporación definirá un plan para la recuperación y continuidad de sus funciones en relación a los datos e información que se respaldan en tiempo real y que son susceptibles de algún riesgo.

5.2.2. Registro de respaldo de información.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 53 de 59

- La dependencia que lidere los procesos tecnológicos de la Corporación se encargará de definir un procedimiento para la administración y control de las copias de seguridad y su cuidado.
- La dependencia que lidere los procesos tecnológicos de la Corporación en conjunto con el administrador del centro de datos deberán:
 - Llevar un registro de las copias de seguridad realizadas con su periodicidad.
 - Identificar las cintas de respaldo y mantener un inventario de estas.
 - Comprobar la integridad de la información.
- La información respaldada deberá ser revisada al menos dos veces al año para garantizar su integridad y disponibilidad.
- La dependencia que lidere los procesos tecnológicos de la Corporación debe verificar los procedimientos de restauración de las copias de seguridad para comprobar su efectividad.
- Se debe contar con los recursos suficientes que permitan identificación de los medios de respaldo de seguridad, datos e información que contiene y ubicación física de estos, de tal manera que sea de fácil y rápido acceso.
- La dependencia que lidere los procesos tecnológicos de la Corporación en sinergia con la administración del data center, aplicará los siguientes procesos:
 - Restaurar por lo menos cada seis meses, el escenario adecuado para probar las copias de respaldo de los Servidores.
 - Configurar la herramienta de ejecución de copias de respaldo para que automáticamente registre el éxito o errores en la ejecución.
 - Validar la integridad y disponibilidad de las cintas de respaldo por lo menos cada cuatro meses.
 - Mantener siempre una copia de la información de los Servidores, para un periodo según lo establecido en el Plan de Continuidad Tecnológica.
 - Se debe mantener un monitoreo frecuente sobre el rendimiento y alcance de la información en la Base de Datos para así asegurar la integridad de la información respaldada.

5.3. Documentación.

- Todas las dependencias de la Corporación serán responsables de mantener documentado y actualizado el Inventario de activos de información. La dependencia que lidere los procesos tecnológicos de la Corporación con el apoyo de Gestión documental, adelantarán labores de consolidación de los activos.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 54 de 59

- Todos los grupos de trabajo y procesos de cada dependencia, deben documentar formalmente las actividades del ejercicio de funciones (manuales, instructivos, guía, entre otros).
- La dependencia que lidere los procesos tecnológicos de la Corporación deberá contar con una gestión de documentos orientados a la gestión estratégica del área y contendrá al menos:
 - Documentación de planeamiento estratégico de TIC para la Corporación conforme al PGAR.
 - Documentación de planes anuales operativos.
 - Documentación sobre solicitudes de servicio recibidas.
 - Documentación de inventario de equipos de cómputo, equipos de telecomunicaciones, periféricos y artefactos tecnológicos.
 - Documentación de inventario de software instalado en equipos.
 - Documentación sobre los mantenimientos sobre los equipos de la entidad.
 - Documentación de licencias de software adquiridas.
 - Documentación de proyectos formalmente desarrollados.
- La dependencia que lidere los procesos tecnológicos de la Corporación hará uso de la documentación formal de la Corporación para la ejecución de los trámites administrativos cuando así se requiera y que estén dentro de los parámetros normativos.
- La dependencia que lidere los procesos tecnológicos de la Corporación adoptará el documento de Políticas generales de los procesos tecnológicos y de seguridad de la información como uno de sus fundamentos para su gestión institucional.

5.4. Daño o destrucción de los activos de información.

Los Activos de Información son susceptibles de diversas situaciones y riesgos que pueden comprometer su estado ideal para ser empleado en los procesos y actividades de la entidad. Entendido lo anterior, la manera de mitigar un evento desfavorable es mediante la aplicación de los lineamientos y políticas de los procesos tecnológicos y de seguridad de la información, igualmente se debe considerar otras disposiciones que aporten a la construcción de lineamientos que amparen los contenidos que reposan y procesan en los activos de información.

- Es deber de toda Corantioquia cuidar, proteger y conservar los activos de información de la entidad.
- Ante el daño o destrucción de un activo de información, se activará el protocolo establecido para la resolución de problemas. Dicho protocolo deberá ser estimado por el propietario o administrador del activo y deberá responder a la reparación inmediata sobre la afectación que se produzca.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
 Municipio: Medellín - Antioquia
 Tel: 57 (4) 493 88 88
 Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 55 de 59

- En relación a cualquier aparato electrónico que almacene datos y vaya a ser desechado, la dependencia que lidere los procesos tecnológicos de la Corporación procederá con la recuperación de información y consignará en un documento formal con los hallazgos y su trámite de disposición final.

5.5. Disposiciones para protección de datos personales.

Las disposiciones para protección de datos personales son las adopciones y aplicabilidad de la norma vigente para la Corporación que se encuentran en concordancia con las Políticas generales de los procesos tecnológicos y de Seguridad de la Información:

- Adopción y aplicación de la Resolución 040-RES1904-1730 de 2019 Por la cual se adopta la política de Protección de Datos Personales para la Corporación Autónoma Regional del Centro de Antioquia Corantioquia.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 56 de 59

6. POLÍTICAS DE HARDWARE

ALCANCE

Garantizar la integridad del recurso tecnológico hardware tales como: servidores, estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, y demás equipos de telecomunicaciones con los que cuenta la entidad.

LINEAMIENTOS:

6.1. Responsabilidad de la gestión con hardware.

- El personal de la dependencia que lidere los procesos tecnológicos de la Corporación será responsable de vigilar por el cuidado y el buen uso del hardware que se encuentre en el data center, armarios y áreas especiales.
- Los equipos de cómputo o de telecomunicaciones serán responsabilidad del usuario a quien se le haya asignado. Este no deberá hacer uso personal de los mismos, al contrario velará por asegurar su cuidado, manteniéndolo limpio y en funcionamiento. De presentarse alguna novedad con el equipo, deberá reportarlo de inmediato a la dependencia que lidere los procesos tecnológicos de la Corporación para su atención y revisión.
- Se establece, que todo equipo o artefacto (hardware) asignado a un usuario es bajo condición de instrumento o herramienta para el cumplimiento de sus labores y, como tal, es propiedad de la Corporación, por tanto no habrá perjuicio de derecho a la privacidad de la información almacenada en estos.
- La dependencia que lidere los procesos tecnológicos de la Corporación definirá e indicará las circunstancias para la sustitución de algún equipo cuando no este en condiciones operativas y funcionales.

6.2. Disposiciones acerca de mantenimiento.

- Es deber de cada usuario informar a la dependencia que lidere los procesos tecnológicos de la Corporación acerca del rendimiento que presente su equipo de cómputo de manera que aporte a la valoración de las situaciones a intervenir para darle solución.
- Es el personal de la dependencia que lidere los procesos tecnológicos de la Corporación los únicos autorizados para adelantar modificaciones o adquisiciones de partes y equipos, igualmente actualizaciones, compras y configuraciones de hardware y software.
- Si se requiere realizar movimientos de equipos dentro o entre las sedes, será la dependencia que lidere los procesos tecnológicos de la Corporación quien coordinará y dispondrá del procedimiento a seguir.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 57 de 59

- Cuando se presente fallas a nivel técnico, la dependencia que lidere los procesos tecnológicos de la Corporación hará una valoración preliminar con el fin de dar solución; de no lograrlo, procederá conforme a los condicionamientos para la reparación o cambio.
- Bajo ninguna circunstancia un equipo de cómputo, equipo de telecomunicaciones, artefacto tecnológico o cualquier otro similar propiedad de Corantioquia no podrá ser abierto, intervenido, reparado, desarmado o cambiado por un usuario, ni mucho menos retirada las cintas de seguridad o garantía que estos traen.
- El usuario conservará en el mejor estado y disposición los elementos periféricos de los equipos; así mismo éstos no podrán ser retirarse o moverse sino es mediante autorización de la dependencia que lidere los procesos tecnológicos de la Corporación.

6.3. Renovación de equipos.

- La Corporación deberá contar con un sistema de información que indique: cantidad de equipos que tiene, datos técnicos e información de mantenimiento realizados. El documento resultado deberá constituirse como la hoja de vida para el equipo, estableciendo su vida útil y el concepto para renovación.
- El concepto de renovación de equipos recae sobre la dependencia que lidere los procesos tecnológicos de la Corporación, el cual deberá proveer un informe donde justifique la solicitud con base en: características de los equipos, tiempo de uso, actividad que desarrolla y por el cual se adquirió, condiciones ambientales del entorno donde se ubica, y demás consideraciones que amplíe y detalle el concepto.
- Desde la dependencia que lidere los procesos tecnológicos de la Corporación se deberá liderar el plan para la adquisición de nuevas tecnologías y equipos, que contribuyan al logro estratégico de los objetivos misionales de la Corporación. En correlación con las dependencias responsable de la aprobación y desembolso del presupuesto para renovación, la dependencia que lidere los procesos tecnológicos de la Corporación, atenderá a los requisitos propios de la formulación para la adquisición de nuevos bienes.
- Corantioquia podrá optar por la renovación de equipo en modalidad leasing considerando las mejores ofertas comerciales, propuestas técnicas y económicas que aprueben la dependencia que lidere los procesos tecnológicos de la Corporación y la Subdirección Financiera. Igualmente se consignará la inclusión de aspecto como: repuestos, mantenimientos, garantías, licencias de software, póliza de seguros y valor agregado del proveedor como extensiones de garantía entre otros.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 58 de 59

6.4. Operación y administración de infraestructura.

- Cada área encargada de la operación y la administración de la infraestructura, contará con cuenta corporativa de uso exclusivo, por la cual se canalizará las actividades propias de sus funciones.
- La infraestructura de red interna de datos es competencia de la dependencia que lidere los procesos tecnológicos de la Corporación, por tanto esta será la encargada de su administración, soporte y gestión. Permitiendo la interconexión de los usuarios y velando por la disponibilidad y funcionamiento. Las disposiciones para acceso y uso de la red están consagradas en el numeral 4.2 correspondiente a Controles de Acceso.
- Toda la infraestructura tecnológica es responsabilidad de la dependencia que lidere los procesos tecnológicos de la Corporación, por tal motivo cualquier acción que tenga que ver con TIC en la Corporación deberá ser tramitada ante esta dependencia.
- Los administradores de la infraestructura monitorearán periódicamente el flujo de sus redes empleado herramientas de monitoreo, seguridad y administración. Con los hallazgos deberán definir planeas que consoliden la función de la red o suprima situaciones adversas.
- La infraestructura de red eléctrica es competencia del área de recursos físicos, o quien haga las funciones de ésta en la Corporación, garantizando el flujo eléctrico constante sin fluctuaciones o cambios de voltaje.
- Está prohibido que cualquier usuario manipule, gestione, altere o intervenga en la red. De ser así, el usuario será responsable de las afectaciones que con sus acciones se generen. Sólo personal autorizado podrá manipular, gestionar e intervenir en las infraestructuras de redes.
- Los usuarios deberán acatar las recomendaciones que desde las áreas de operación e infraestructura se dicten cuando estén en función de la atención, corrección o prevención de una situación que pueda afectar el normal funcionamiento de las actividades dentro de la Corporación.

6.5. Inventario y reparación de equipos.

- Todos los equipos tecnológicos, de cómputo y de telecomunicaciones, y demás partes de la infraestructura tecnológica, serán recepcionadas por el área de almacén, quienes mediante las técnicas y procedimientos para inventariar los bienes de la Corporación marcarán, identificarán e individualizarán los equipos y las partes para su correspondiente

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88
Correo electrónico: corantioquia@corantioquia.gov.co

 CORANTIOQUIA	SISTEMA DE GESTIÓN INTEGRAL - SGI		
	RESOLUCIÓN		
	CÓDIGO: FT-GIC-24	VERSIÓN: 03	PÁGINA: 59 de 59

control, dejándolo a disposición a la dependencia que lidere los procesos tecnológicos de la Corporación.

- La dependencia que lidere los procesos tecnológicos de la Corporación gestionará, custodiará y alimentará el inventario de equipos de cómputo y equipos de telecomunicaciones con el mayor detalle de información de estos mediante un software de gestión. Dicho inventario deberá ser actualizado de manera permanente. Una vez al año, el inventario se realizará de pared a pared en todas las sede de la Corporación incluyendo la sede central y, generando informes sobre el asunto.
- Desde la dependencia que lidere los procesos tecnológicos de la Corporación se deberá garantizar, mediante dispositivos de seguridad, la integridad de los equipos que estan bajo responsabilidad de los usuarios. Para ello deberá proceder con bloqueos de puertos y sellamiento de partes para evitar intrusiones, daños y malos usos.
- Los dispositivos de seguridad empleados por la dependencia que lidere los procesos tecnológicos de la Corporación no podrán ser alterados, removidos o dañados, excepto por el personal del área que esté realizando una actividad y que obligatoriamente daba proceder para la labor, debiendo, una vez finalizada la reposición nuevamente del dispositivo de seguridad. En todo caso, el personal del área deberá dejar un informe de su gestión y justificación de su labor realizada.
- La dependencia que lidere los procesos tecnológicos de la Corporación deberá establecer el procedimiento y los tiempos a seguir para la implementación y control de los servicios de reparación, situación que deberá ser acatada por todos los usuarios.
- Los sobrecostos que den a lugar, en una reparación, como resultado de algún daño no incluido en garantía, debe estar a cargo de la Subdirección Administratia o Grupo Interno de Trabajo.
- Será competencia de la dependencia que lidere los procesos tecnológicos de la Corporación la administración del presupuesto destinado a la compra de repuestos, accesorios y partes de equipos y artefactos tecnológicos de la entidad, demostrando su viabilidad presupuestal y técnica.
- Será responsabilidad de la dependencia que lidere los procesos tecnológicos de la Corporación la gestión de garantías de equipos y artefactos tecnológicos. Si alguno de estos no cuenta con garantía, la dependencia que lidere los procesos tecnológicos de la Corporación procederá con la gestión de reparación del mismo o el envío a centros especializados para dar solución al problema. El área usuaría deberá asumir los sobrecostos y, la dependencia que lidere los procesos tecnológicos de la Corporación gestionará las condiciones valorando la viabilidad presupuestal y técnica de la solución.

Corantioquia está comprometida con el tratamiento legal, lícito, confidencial y seguro de sus datos personales. Por favor consulte nuestra Política de Tratamiento de datos personales en nuestra página web: www.corantioquia.gov.co



Dirección: Carrera 65 # 44ª-32
Municipio: Medellín - Antioquia
Tel: 57 (4) 493 88 88

Correo electrónico: corantioquia@corantioquia.gov.co