REGIÓN CENTRAL
RAP-E | Estamos Construyendo Región

POLITICA DE SEGURIDAD DE LA INFORMACIÓN DIGITAL

REGIÓN ADMINISTRATIVA Y DE PLANEACIÓN ESPECIAL

RAP-E Región Central

Dirección Administrativa y Financiera
Proceso TICs
2025

BOGOTÁ BOYACÁ CUNDINAMARCA META TOLIMA HUILA

REGIÓN CENTRAL
RAP-E | Estamos Construyendo Región

TABLA DE CONTENIDO

1 INTRODUCCIÓN

La información constituye un activo estratégico y esencial para la Región Administrativa y de Planeación Especial – RAP-E Región Central, ya que soporta la toma de decisiones, el desarrollo de procesos misionales y la prestación eficiente de los servicios a la ciudadanía. En el actual entorno digital, caracterizado por la transformación tecnológica y el aumento de las amenazas cibernéticas, la protección de la información se convierte en un factor crítico para garantizar la confianza institucional, la transparencia y la continuidad del servicio público.

En este contexto, la RAP-E Región Central presenta la Política de Seguridad Digital, la cual se encuentra alineada con la Política de Seguridad de la Información de la Entidad y con los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, que constituye el marco habilitador del Gobierno Digital en Colombia.

La política establece directrices, principios y compromisos que orientan a servidores públicos, contratistas y terceros en la gestión y protección de la información, asegurando su confidencialidad, integridad, disponibilidad y trazabilidad, en cumplimiento de la normativa nacional y de estándares internacionales de buenas prácticas.

Con su implementación, la RAP-E Región Central ratifica su compromiso con la seguridad digital, la protección de datos personales, el respeto al Habeas Data, el resguardo del secreto empresarial, y la construcción de una cultura organizacional orientada a la prevención, el control y la mejora continua en materia de seguridad de la información.

2 OBJETIVOS

1. Establecer lineamientos que permitan enfrentar el incremento de amenazas informáticas y los retos en materia de ciberseguridad, con el fin de que el Proceso de Gestión TICs adelante las acciones necesarias para mitigar los riesgos que puedan generar afectaciones legales, financieras, operativas o de imagen a la RAP-E Región Central.

2. Implementar controles orientados a garantizar la confidencialidad, integridad, disponibilidad y trazabilidad de la información administrada por la Entidad.

3. Asegurar el cumplimiento de los requerimientos legales y regulatorios aplicables en materia de protección y privacidad de la información, de acuerdo con la normatividad vigente y las directrices nacionales de MinTIC.

4. Promover la mejora continua de los procesos institucionales y de la atención a los usuarios, mediante la identificación, valoración y tratamiento de riesgos sobre los activos de información, garantizando una respuesta oportuna y eficaz a los requerimientos.

5. Mantener actualizados los lineamientos de seguridad de la información digital, asegurando su pertinencia, vigencia, eficacia y alineación con las orientaciones estratégicas de la RAP-E Región Central.

6. Incentivar, sensibilizar y monitorear la aplicación de buenas prácticas por parte de todos los colaboradores, promoviendo el adecuado tratamiento, resguardo y protección de la información institucional.

7. Robustecer las capacidades de la RAP-E Región Central para identificar, proteger, detectar, responder y recuperar ante incidentes o ataques de ciberseguridad, contribuyendo a la resiliencia organizacional.

3 ALCANCE

La presente Política establece los lineamientos para la gestión de la seguridad de la información digital que el Proceso de Gestión TICs recolecta, procesa, almacena, administra y transmite en desarrollo de sus funciones.

Su aplicación es de carácter obligatorio para todos los servidores públicos, contratistas, proveedores y terceros que, de manera directa o indirecta, tengan acceso a los activos de información de la Entidad, sin importar el medio, formato, ubicación o etapa del ciclo de vida en la que se encuentren dichos activos (creación, procesamiento, almacenamiento, transmisión, uso o eliminación).

Asimismo, el alcance comprende la adopción de medidas técnicas, administrativas, jurídicas y organizacionales que permitan proteger la información institucional frente a amenazas internas y externas, garantizando su confidencialidad, integridad, disponibilidad y trazabilidad, en coherencia con los lineamientos del MSPI y las directrices estratégicas de la RAP-E Región Central.

Excepciones: Esta política no aplica a información pública cuya gestión y acceso estén regulados por otras normas de transparencia, ni al uso de plataformas externas que no sean administradas por la Entidad.

4 DESCRIPCIÓN DE LA POLÍTICA

La Política de Seguridad de la Información Digital de la Región Central – RAP-E establece los lineamientos institucionales orientados a garantizar una adecuada gestión de la información en el marco de sus funciones misionales. La Entidad reconoce la información como un activo estratégico y, en consecuencia, se compromete con el establecimiento, implementación y mejora continua de la Seguridad de la Información Digital, la Protección de Datos Personales y la Continuidad de Negocio.

Este compromiso incluye la adopción de mecanismos para identificar, evaluar y mitigar los riesgos asociados a la gestión de información, que comprenden la generación, integración, levantamiento, compilación, validación, almacenamiento y suministro de información institucional y regional, en cumplimiento de los deberes con las Entidades Territoriales Asociadas y demás partes interesadas, en concordancia con la misión y visión de la RAP-E.

La presente política establece directrices para proteger, recuperar y conservar la información digital, asegurando su confidencialidad, integridad, disponibilidad, trazabilidad, interacción y usabilidad a lo largo del tiempo. Promueve la consolidación de una cultura de seguridad digital orientada a salvaguardar los datos personales, la propiedad intelectual y el patrimonio de información de la Entidad.

Como fundamento normativo y estratégico, la política se basa en:

- CONPES 3854 de 2016: Política Nacional de Seguridad Digital, que establece un marco estratégico para la gestión de riesgos de seguridad digital en Colombia.

- CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital, que fortalece la gobernanza en seguridad digital y la protección de datos personales.

- CONPES 3701: Lineamientos de Política para Ciberseguridad y Ciberdefensa, que orienta la respuesta ante amenazas cibernéticas.

- Lineamientos del Ministerio TIC y el MSPI: Que proporcionan directrices para la gestión de la seguridad y privacidad de la información en las entidades públicas.

Con ello, la RAP-E garantiza que su Política de Seguridad Digital se encuentra alineada con la normativa nacional vigente y las mejores prácticas internacionales, asegurando la protección integral de sus activos de información y la continuidad de sus operaciones.

5 MARCO LEGAL Y/O NORMATIVO

La Región Administrativa y de Planeación Especial – RAP-E, en cumplimiento de sus funciones y responsabilidades en la gestión de la información, se adhiere al marco legal y normativo vigente en Colombia, orientado a la protección de los activos de información, la seguridad digital y la protección de datos personales.

ACTO ADMINISTRATIVO	OBJETO
Constitución Política de Colombia, 1991 – Artículo 15	Reconoce el derecho de todas las personas a la intimidad personal y familiar, al buen nombre, y establece la obligación del Estado de proteger estos derechos, incluyendo la posibilidad de conocer, actualizar y rectificar la información contenida en bancos de datos y archivos de entidades públicas y privadas.
Ley 527 de 1999	Regula el acceso y uso de mensajes de datos, comercio electrónico, firmas digitales y entidades de certificación.
Ley 594 de 2000	Ley General de Archivos, reglamentada parcialmente por los Decretos 4124 de 2004 y 1100 de 2014.
Ley 603 de 2000	Protección de los derechos de autor, incluyendo el software como activo y la obligación de declarar la legalidad de los programas utilizados.
Ley 962 de 2005	Simplificación y racionalización de trámites; establece atributos de seguridad en la información electrónica de entidades públicas.
Ley 1150 de 2007	Seguridad de la información electrónica en la contratación en línea.

Ley 1266 de 2008	Disposiciones generales sobre Hábeas Data, manejo de bases de datos personales financieras, comerciales y de servicios.
Ley 1273 de 2009	Modificación del Código Penal, creación del bien jurídico "protección de la información y los datos", y preservación integral de sistemas que utilizan TIC.
Ley 1341 de 2009	Principios de la sociedad de la información y organización de las TIC; creación de la Agencia Nacional del Espectro.
Ley 1437 de 2011	Código de Procedimiento Administrativo y Contencioso Administrativo; uso de medios electrónicos en el procedimiento administrativo.
Ley 1474 de 2011 / Decreto 4632 de 2011	Fortalecimiento de mecanismos de prevención, investigación y sanción de actos de corrupción y regulación de comisiones de control.
Ley 1581 de 2012	Régimen general de protección de datos personales.
Decreto 2364 de 2012	Reglamenta la firma electrónica.
Decreto 2609 de 2012	Reglamenta parcialmente la Ley 594 de 2000 y artículos de la Ley 1437 de 2011 sobre gestión documental.

- ## ESTÁNDARES INTERNACIONALES COMPLEMENTARIOS

Se adoptan lineamientos de ISO/IEC 27001 e ISO/IEC 27002:2022 para la gestión de seguridad de la información, aplicando controles actualizados según mejores prácticas internacionales.

Se aplican lineamientos de ISO 22301 para la continuidad del negocio, asegurando la resiliencia y la recuperación ante incidentes que afecten la operación institucional.

Con esto, la RAP-E Región Central garantiza que su política de seguridad digital no solo cumple con la normativa nacional vigente, sino que también incorpora estándares internacionales de buenas prácticas para la gestión integral de la información y la continuidad operativa.

- ## COMPROMISO DE LA RAP-E

La RAP-E Región Central se compromete a garantizar la confidencialidad, integridad, disponibilidad y seguridad de la información que gestiona. Para ello, se realizan:

- Identificación y tratamiento de riesgos asociados a los activos críticos de información.
- Seguimiento permanente de las acciones de seguridad, de acuerdo con la gestión de riesgos establecida en el Sistema Integrado de Gestión.
- Implementación de controles, procedimientos y medidas de mejora continua que aseguren el cumplimiento de la normativa vigente y la protección de los datos institucionales y personales.

Con ello, la RAP-E Región Central asegura que la gestión de la información se realiza en un marco legal robusto, alineado con los lineamientos nacionales de seguridad digital, protección de datos y continuidad de negocio.

6 MATRIZ RACI – POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DIGITAL

Con el fin de definir con precisión los roles y responsabilidades en la implementación, seguimiento y mejora de la Política de Seguridad de la Información Digital, se presenta la siguiente matriz RACI. Esta herramienta permite identificar quién es responsable (R), quién aprueba (A), quién debe ser consultado (C) y quién debe ser informado (I) en cada actividad clave, promoviendo una gestión clara, colaborativa y eficiente de la seguridad digital en la RAP-E Región Central.

Actividad / Proceso	R (Responsable)	A (Aprobador)	C (Consultado)	I (Informado)
Formulación y actualización de la política	Proceso Gestión TICs	Comité Institucional de Gestión y Desempeño	Asesoría Jurídica / Oficina Asesora de Planeación Institucional	Todos los colaboradores
Implementación de controles técnicos	Proceso Gestión TICs	Comité Institucional de Gestión y Desempeño	Proveedores tecnológicos / Asesoría Jurídica	Gerencia / Oficina Asesora de Planeación Institucional
Capacitación y sensibilización en seguridad digital	Proceso Gestión TICs / Gestión de Talento Humano y Bienestar	Dirección Administrativa y Financiera	Asesoría de Comunicaciones	Todos los colaboradores
Gestión de incidentes de seguridad digital	Proceso Gestión TICs	Comité Institucional de Gestión y Desempeño	CSIRT Nacional / ColCERT	Gerencia / Áreas afectadas / Asesoría Jurídica
Revisión normativa Anual	Asesoría Jurídica / Proceso Gestión TICs	Comité Institucional de Gestión y Desempeño	Asesoría Jurídica / Proceso Gestión TICs	Dirección Administrativa y Financiera
Auditoría interna de cumplimiento	Asesoría de Control Interno	Comité Institucional de Gestión y Desempeño	Proceso Gestión TICs / Gestión de Talento Humano y Bienestar	Gerencia / Oficina Asesora de Planeación Institucional
Firma de acuerdos de confidencialidad	Gestión de Talento Humano y Bienestar	Comité Institucional de Gestión y Desempeño	Asesoría Jurídica / Proceso Gestión TICs	Contratistas / Terceros / funcionarios

Publicación de documentos en la web institucional	Asesoría de Comunicaciones	Dirección Administrativa y Financiera	Proceso Gestión TICs / Asesoría Jurídica	Ciudadanía / Entidades externas
Inclusión en grupos institucionales de WhatsApp	Gestión de Talento Humano y Bienestar / Gerencia	Dirección Administrativa y Financiera	Asesoría Jurídica / Proceso Gestión TICs	Colaboradores autorizados

7 RESPONSABLES DE LA POLÍTICA

7.1 RESPONSABLES INTERNOS

7.1.1 Formulación y Actualización

El Proceso de Gestión de TICs es responsable de:

- Elaborar, mantener y actualizar el presente manual, asegurando la participación de todas las áreas que intervienen en la gestión de la información digital.
- Recibir reportes y registrar las detecciones de incumplimiento frente a los lineamientos establecidos, analizando su naturaleza y recurrencia, y determinando las acciones correspondientes para su escalamiento al nivel directivo. Esto incluye la gestión de fallas o riesgos que se materialicen en materia de Seguridad de la Información Digital, a fin de que la instancia competente determine las medidas correctivas necesarias.
- Garantizar que lo establecido en el Política de Seguridad de Información Digital sea complementario al Manual de Gestión de TIC, integrándose como parte de la cultura organizacional. Todos los colaboradores, contratistas y proveedores vinculados a la Región Central deben conocer y cumplir con las condiciones y lineamientos establecidos.

7.1.2 Implementación

Todos los Todos los colaboradores de la RAP-E Región Central deben recibir una inducción inicial en Seguridad de la Información Digital y en la gestión de la información institucional, complementada con procesos de entrenamiento y sensibilización periódica que permitan reforzar los lineamientos, políticas y procedimientos definidos por la Entidad. Estas acciones buscan garantizar que el personal conozca y aplique adecuadamente las disposiciones establecidas, contribuyendo a la protección integral de los activos de información.

En el marco de dichos procesos formativos, se debe informar a los colaboradores acerca de los riesgos comunes de seguridad digital a los que se expone la Entidad, los requerimientos normativos y lineamientos internos que deben cumplirse, así como sus deberes, derechos y responsabilidades frente al incumplimiento de la política. De igual manera, se brindará capacitación relacionada con el uso seguro de los activos de información y de los recursos tecnológicos institucionales, promoviendo una cultura organizacional basada en la protección y el manejo responsable de la información.

Las labores de inducción, sensibilización y entrenamiento estarán a cargo del Proceso Gestión TICs, con el apoyo del Proceso de Gestión del Talento Humano y de Comunicación Institucional, utilizando medios de divulgación como correo electrónico, Intranet, carteleras, materiales audiovisuales, reuniones y actividades presenciales, entre otros.

7.1.3 Seguimiento

El Comité Institucional de Gestión y Desempeño articula los esfuerzos, recursos, metodologías y estrategias para asegurar la implementación de la política, de acuerdo con lo dispuesto en:

- Artículo 2.2.22.3.8 del Decreto 1499 de 2017.
- Artículo 5 de la Resolución 383 de 2017.

Entre sus funciones principales se encuentran:

- Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.
- Actuar como instancia orientadora de la Estrategia de Gobierno en Línea, de conformidad con el parágrafo 1 del artículo 8 del Decreto 2573 de 2014.

7.2 RESPONSABLES EXTERNOS

Para fortalecer las prácticas y controles de seguridad de la información digital, la RAP-E Región Central buscará establecer relaciones de cooperación y asesoramiento con las siguientes entidades:

- Superintendencia de Industria y Comercio (SIC).
  - **Correo electrónico:** contactenos@sic.gov.co
  - **Teléfono fijo Bogotá:** (601) 592 0400
  - **Línea gratuita nacional:** 018000-910165
- Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).
  - **Correo electrónico de mesa sectorial:** mesadeserviciosectorial@mintic.gov.co
  - **Teléfono Bogotá:** (601) 344 3460
  - **Extensiones:** 3325, 3215, 3499
- ColCERT – Grupo de Respuesta a Emergencias Cibernéticas.
  - **Correo electrónico:** colcert@mintic.gov.co
  - **Teléfono MinTIC:** (601) 344 3460
- CSIRT de la Policía Nacional.
  - **Correo electrónico:** delitos.tecnologicos@policia.gov.co
  - **Teléfono DIJIN:** (601) 426 6900
- CSIRT de Gobierno.
  - **Correo electrónico:** csirtgob@mintic.gov.co
  - **Teléfono MinTIC:** (601) 344 3460

- Unidad de Delitos Informáticos – DIJIN.
  - **Correo electrónico:** dijin.delitosinformaticos@policia.gov.co
  - **Teléfono DIJIN:** (601) 426 6900

8 ARTICULACIÓN CON EL MIPG Y EL SIG

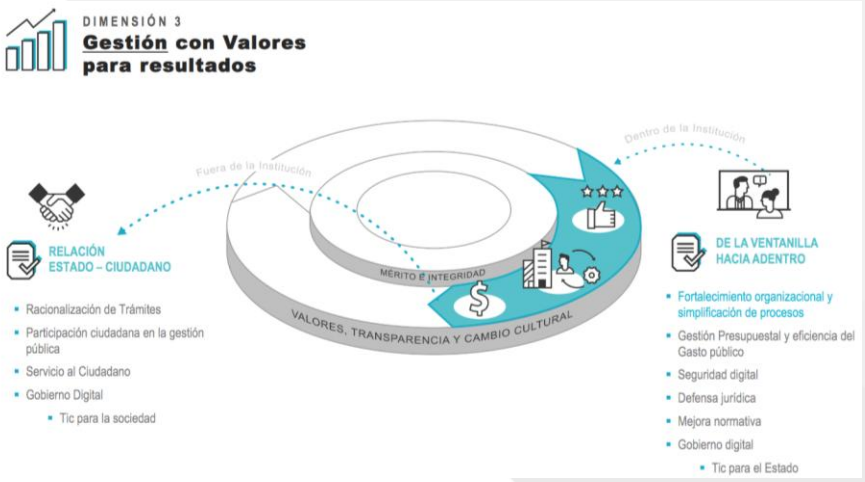
8.1 ARTICULACIÓN CON EL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN (MIPG)

La Política de Seguridad de la Información Digital se encuentra alineada con el Modelo Integrado de Planeación y Gestión (MIPG), incorporando los principios de la Dimensión 3: Gestión con Valores para Resultados, que busca garantizar que la organización cumpla sus funciones y logre los resultados previstos, respetando los valores del servicio público.

Para tal fin, la política se orienta a atender los aspectos estratégicos, operativos y de control que permiten asegurar la eficiencia, transparencia, integridad y seguridad de la información en todos los procesos institucionales. Esta dimensión se entiende desde dos perspectivas complementarias:

- Gestión interna o “de la ventanilla hacia adentro”: Enfocada en asegurar la correcta operación de la organización, incluyendo la planificación, el control de riesgos, la protección de activos de información, el cumplimiento de procedimientos y la mejora continua de los procesos.

- Relación Estado-Ciudadano: Orientada a garantizar la transparencia, disponibilidad y confiabilidad de la información frente a los ciudadanos y las partes interesadas, fortaleciendo la confianza pública y facilitando la prestación eficiente de los servicios institucionales.



De esta manera, la política no solo asegura la protección de los activos de información, sino que también contribuye al cumplimiento de la misión institucional, la toma de decisiones basada en información confiable y la consolidación de una cultura de gestión con valores y resultados.

8.2 ARTICULACIÓN CON EL SIG

La Política de Seguridad de la Información Digital se encuentra articulada al Sistema Integrado de Gestión (SIG) de la RAP-E Región Central así:

PROCESOS	DOCUMENTOS
PR-12. Gestión TIC	M-GT.01-01 Manual de Gestión de TIC M-GT.01.02 Manual de Seguridad de la Información Digital.
INTERACCIÓN CON OTROS PROCESOS	
PR-02. Administración del SIG	P-SIG.03 Administración y Gestión del Riesgo
PR-04. Servicio al Ciudadano	P-GD.01 Gestión de PQRSD Política de Tratamiento de Datos
PR-07. Gestión de Bienes y Servicios	P-GBS.01. Administración de bienes e insumos. P-GBS.02. Administración de servicios de funcionamiento P-GBS.03. Administración de seguros
PR-10. Gestión del Talento Humano	P-GTH.11 Ciclo de Vida de los Colaboradores F-GTH.10.4 Acta de compromiso seguridad de la información y protección de datos personales
PR-11. Gestión de Contratación	Manual de Contratación F-M-GC.01-08. Aprobación de garantía
PR.13. Planificación, Gestión y Ejecución de Proyectos	P-PGEP.02 Elaboración de Productos Cartográficos

9 LINEAMIENTOS GENERALES

9.1 DISPONIBILIDAD A NIVEL DE USUARIO FINAL

Grupos de Interés	Usuarios finales de tecnologías de información.
	Administradores de Tecnologías de Información
Lineamiento General: El Proceso de Gestión TICs está comprometida con el buen uso de los recursos de procesamiento de la información, por ello, brindará lineamientos en la materia, que deben ser conocidos y cumplidos por los usuarios finales y administradores de tecnologías de información.	

9.1.1 SERVICIOS DE USUARIO FINAL Y SUPERFICIE DE TRABAJO

A. Computadores Asignados

A los colaboradores de la RAP-E Región Central, en algunos casos, se les proporciona en calidad de préstamo un equipo de cómputo para el cumplimiento de sus responsabilidades. Dicho equipo puede ser de escritorio o portátil, y se asignará una vez legalizado el contrato o la vinculación con la Entidad.

Tras la entrega, los colaboradores son responsables de todos los elementos que forman parte del equipo asignado, teclado, mouse, pantalla, entre otros.

La configuración, instalación, desinstalación y mantenimiento del hardware, así como del software operativo, base, de aplicación y utilitario de los equipos de cómputo y de los dispositivos periféricos (como impresoras o escáneres), así como de los equipos de comunicaciones (router, switch, access point), son responsabilidad exclusiva del Proceso de Gestión TICs. Solo este grupo está autorizado para realizar dichos procedimientos.

En general, los usuarios deben cumplir con las siguientes disposiciones:

a) No causar daños a los equipos de cómputo.
b) No insertar objetos extraños en las ranuras de los equipos.
c) No instalar programas sin la autorización previa del área de Gestión TICs la Información.
d) No realizar ninguna actividad de mantenimiento de hardware o software.

B. Bloqueo de Pantalla

En el marco del Proceso de Gestión de TICs, es fundamental reducir el riesgo de pérdida o fuga de información por el uso no autorizado de los sistemas. Por ello, se requiere que los equipos de cómputo permanezcan protegidos, incluso cuando el usuario no esté frente a ellos.

Cada colaborador puede bloquear su sesión al alejarse del computador utilizando la combinación de teclas **Ctrl+Alt+Suprimir o Inicio (Windows) + L**.

Adicionalmente, para prevenir situaciones en las que la estación de trabajo quede desatendida y sin bloqueo, los equipos cuentan con un bloqueo automático tras 5 minutos de inactividad. Esta medida complementa, pero no reemplaza, la responsabilidad del colaborador de mantener su estación de trabajo y su espacio bajo control en todo momento.

9.1.2 CÓDIGO MALICIOSO Y USO LEGAL DE SOFTWARE

A. Código Malicioso

Los usuarios deben aplicar de manera constante medidas preventivas para evitar la presencia de código malicioso (virus, troyanos, spyware, entre otros) en los computadores de la Región Central. Para ello, deben estar atentos a las notificaciones y recomendaciones que el área de Gestión TICs emita sobre riesgos de virus provenientes de Internet, correo electrónico, otros computadores de la red o dispositivos de almacenamiento extraíbles.

Todos los equipos de cómputo deben contar siempre con software antivirus instalado, configurado, habilitado, actualizado y en funcionamiento, siendo esta responsabilidad del área de Gestión TICs. La instalación, modificación de configuración y verificación del funcionamiento del antivirus son exclusivas del personal de este grupo, y ningún usuario debe intentar realizar estas acciones por su cuenta.

Asimismo, ningún usuario debe intentar eliminar código malicioso sin la asistencia del Grupo de TICs. Si un colaborador sospecha que su equipo asignado o algún dispositivo autorizado está infectado, debe suspender inmediatamente cualquier actividad, desconectar el equipo de la red y reportar la situación al Grupo de TICs. El equipo sólo podrá volver a ser utilizado una vez el Grupo de TICs haya dado el tratamiento correspondiente al incidente.

La alta gerencia proveerá los recursos necesarios para adquirir, mantener y actualizar las herramientas tecnológicas que permitan identificar, controlar y mitigar las amenazas informáticas.

B. Uso Legal de Software

Todo el software utilizado en la RAP-E Región Central es adquirido legalmente y cumple con las leyes de protección de derechos de autor. Por lo tanto, no está permitido que los usuarios descarguen o instalen software por su cuenta, incluyendo aquel de libre distribución.

Si un colaborador requiere la instalación de algún software para cumplir con sus funciones, debe solicitarlo al Grupo de TICs, quien evaluará y realizará la instalación de manera autorizada.

9.1.3 USO DEL CORREO ELECTRÓNICO

A. Asignación de Cuentas y Monitoreo

Los colaboradores que disponen de correo electrónico institucional, considerado una herramienta de comunicación oficial, deben destinarlo exclusivamente a fines institucionales. El Proceso de Gestión de TIC se reserva el derecho de acceder, utilizar y gestionar la información contenida en las cuentas de correo, bien sea para atender requerimientos de orden judicial, administrativo o de cualquier otra índole exigida por la ley, o para verificar el correcto uso del servicio.

En caso de que el usuario utilice el correo institucional para fines distintos a los señalados, el Proceso de Gestión de TICs estará autorizado a utilizar, almacenar o suprimir la información, sin que el titular pueda alegar perjuicio o solicitar compensación. El uso del correo institucional con fines personales constituye una autorización tácita del usuario para que el Proceso de Gestión de TICs trate dicha información.

B. Uso del Correo Electrónico

1. Responsabilidad del contenido:

   El usuario remitente es responsable del contenido, veracidad y legalidad de la información transmitida a través de los sistemas de mensajería y correo institucional, de conformidad con los principios de confidencialidad, integridad y disponibilidad de la información.

   Al reenviar mensajes o documentos, el usuario deberá preservar la integridad de la información, absteniéndose de alterar, modificar o eliminar los datos originales, metadatos o archivos adjuntos, salvo autorización expresa.

   Todo documento remitido deberá enviarse en formatos seguros y estandarizados, preferiblemente PDF, o mediante archivos protegidos con mecanismos de seguridad (por ejemplo, control de edición, cifrado o contraseñas), garantizando:

   - La integridad de la información,
   - La correcta visualización del contenido,
   - La protección contra accesos no autorizados.

   El incumplimiento de estas disposiciones constituye una violación a la Política de Seguridad de la Información y podrá dar lugar a las acciones administrativas, disciplinarias o legales correspondientes.

2. Prohibiciones:

- Contenido inapropiado:

  No se permite crear, enviar, retransmitir o almacenar mensajes que contengan contenido ofensivo, difamatorio, discriminatorio, sexualmente explícito o que promueva un ambiente hostil, basado en criterios

como raza, género, nacionalidad, orientación sexual, religión, ideología política, apariencia física, estrato socioeconómico o discapacidad.

- Mensajes masivos y cadenas:
  Está prohibido generar, reproducir o enviar cadenas de mensajes, correos masivos no autorizados o comunicaciones similares, ya que pueden:

  - Propagar código malicioso (virus, troyanos u otros),
  - Saturar el tráfico de los sistemas de correo institucional,
  - Generar riesgos de seguridad de la información,
  - Facilitar prácticas de *spam*, *phishing* u otros mecanismos de fuga de información.

- Respeto a la desconexión laboral:
  En cumplimiento de la normativa vigente sobre desconexión laboral, el envío de comunicaciones institucionales deberá realizarse exclusivamente dentro del horario laboral establecido, salvo situaciones excepcionales debidamente justificadas. No se permitirá el uso de los sistemas de mensajería o correo institucional para exigir, directa o indirectamente, respuestas o actividades fuera de la jornada laboral.

3. Advertencias y configuraciones de seguridad:

   El Proceso de Gestión de TICs configurará advertencias de seguridad estándar en todos los mensajes dirigidos a destinatarios externos, indicando al menos que:

   - El mensaje puede contener información confidencial.
   - Está destinado únicamente a los destinatarios autorizados.
   - La retención, difusión, distribución o copia indebida está prohibida y sancionada por la ley.
   - Las opiniones expresadas son del autor y no necesariamente reflejan las de la RAP-E Región Central.

4. Archivos adjuntos:
   Aunque las herramientas institucionales, como el antivirus, analizan los archivos adjuntos en busca de código malicioso, no se deben descargar archivos de remitentes desconocidos o sospechosos.

5. Disclaimer obligatorio en correos electrónicos:
   Todos los mensajes enviados a través del correo corporativo deberán incluir el siguiente aviso de confidencialidad:

   ***NOTA CONFIDENCIAL**: "La información contenida en esta comunicación es confidencial y solo puede ser utilizada por la persona natural o jurídica a la cual está dirigida. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia de este mensaje, se encuentra prohibida y sancionada por la ley. Si por error recibe este mensaje, favor reenviar y borrar el mensaje recibido inmediatamente." (Numeral 5º del Artículo 3º de la Resolución del Archivo General de la Nación No. 089 de 2003- Reglamento para el uso de Internet y Correo Electrónico)".*

9.1.4 AUTORIZACIÓN PARA INCLUSIÓN EN GRUPO DE WHATSAPP INSTITUCIONAL

De conformidad con lo dispuesto en la Ley 1581 de 2012 y el Decreto 1377 de 2013, todo tratamiento de datos personales requiere el consentimiento previo, expreso e informado del titular. En consecuencia, para ser incluido en el grupo de WhatsApp institucional de la RAP-E Región Central, el titular deberá diligenciar y firmar el formato de autorización para la inclusión en el grupo de WhatsApp institucional, el cual constituye la evidencia de la autorización otorgada.

El tratamiento de los datos personales asociados al uso del grupo de WhatsApp institucional se realizará bajo los principios de confidencialidad, integridad y disponibilidad, en concordancia con la Política de Seguridad de la Información de la Entidad y los lineamientos establecidos en la norma ISO/IEC 27001:2022, particularmente en lo relativo al uso aceptable de activos de información y la protección de la información personal.

El grupo de WhatsApp institucional tendrá como finalidad exclusiva la divulgación de información de carácter institucional y operativo, y su utilización estará estrictamente limitada al horario laboral establecido, en observancia del derecho a la desconexión laboral. No se permitirá el envío de mensajes, solicitudes o requerimientos fuera de la jornada laboral, salvo situaciones excepcionales debidamente justificadas y autorizadas.

La participación en el grupo de WhatsApp institucional es de carácter voluntario y no constituye una obligación para servidores públicos, contratistas o colaboradores. En los casos en que el titular no otorgue la autorización o no entregue el formato debidamente firmado, la información institucional deberá ser enviada por medio del correo electrónico institucional, garantizando el acceso oportuno a la información sin vulnerar los derechos del titular.

El incumplimiento de estas disposiciones, así como el tratamiento de datos personales sin la debida autorización, será considerado una violación a la Política de Seguridad de la Información y podrá dar lugar a sanciones administrativas, disciplinarias y legales, conforme a la normativa vigente y a los controles definidos en el Sistema de Gestión de Seguridad de la Información (SGSI).

9.1.5 PUBLICACIÓN DE DOCUMENTOS EN LA PÁGINA WEB INSTITUCIONAL

De acuerdo con lo dispuesto en la Ley 1712 de 2014 –Ley de Transparencia y del Derecho de Acceso a la Información Pública– y el Decreto 1081 de 2015, la Entidad deberá garantizar que la información publicada en su página web institucional se presente en formatos accesibles, estandarizados y de fácil consulta.

Por lo anterior, todo documento que se publique en la página web de la Entidad deberá estar en formato preferiblemente PDF, o mediante archivos protegidos con mecanismos de seguridad (por ejemplo, control de edición, cifrado o contraseñas), asegurando su integridad, portabilidad y consulta, en cumplimiento de los

lineamientos de transparencia activa y acceso a la información pública. Queda expresamente prohibida la publicación de documentos o información en formatos editables.

9.1.6 ACUERDOS DE CONFIDENCIALIDAD PARA FUNCIONARIOS, CONTRATISTAS Y TERCEROS

En cumplimiento de lo dispuesto en la Ley 1581 de 2012 (Protección de Datos Personales), la Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información Pública), y el Decreto 1078 de 2015 (Política de Gobierno Digital y Seguridad de la Información), la Entidad deberá garantizar la confidencialidad, integridad y disponibilidad de la información a la que tengan acceso los funcionarios, contratistas y terceros que presten servicios.

Por lo anterior, todo contrato, orden de prestación de servicios, vinculación laboral o participación de terceros deberá estar respaldado por la firma de un Acuerdo de Confidencialidad de la Información, en el cual se establezca expresamente:

- La prohibición de divulgar, modificar, alterar o utilizar la información de la Entidad con fines no autorizados.
- La obligación de custodiar y proteger los datos personales, documentos y activos de información conforme a la normatividad vigente.
- La permanencia del deber de confidencialidad incluso después de finalizada la relación contractual, laboral o de prestación de servicios.

El diligenciamiento y firma del Formato de Acuerdo de Confidencialidad será un requisito obligatorio previo a la ejecución de actividades, contratos o prestación de servicios con la Entidad.

El incumplimiento de esta obligación dará lugar a las sanciones contractuales, disciplinarias, administrativas o legales que correspondan.

9.1.7 USO DE INTERNET INSTITUCIONAL

La Región Central RAPE, con el objetivo de apoyar el desarrollo de las actividades institucionales, proporciona acceso a Internet a sus colaboradores. Considerando que los recursos de la Entidad deben ser optimizados, los usuarios deben hacer un uso responsable y racional del servicio.

El Proceso de Gestión de TICs es responsable de proponer perfiles de acceso y establecer reglas de control de contenido en la navegación, incluyendo la regulación del acceso a sitios de alto consumo de ancho de banda, juegos y otras páginas especiales.

- Prohibiciones y restricciones:

- No está permitido el acceso a sitios pornográficos, con especial énfasis en aquellos que involucren pornografía infantil, contenido erótico u obsceno, ni a sitios de terrorismo.
- La utilización de chat, mensajería instantánea, y la descarga de música, radio o video en vivo es discrecional y queda sujeta al consumo de recursos de la red, pudiendo requerir autorización del Proceso de Gestión de TICs.
- Debido a la obligación legal de usar software licenciado y a la protección de los derechos de propiedad intelectual, los usuarios no deben descargar, almacenar o utilizar en la plataforma tecnológica de la RAP-E Región Central software, música, libros, publicaciones, videos u otro material protegido por derechos de autor, sobre el cual la Entidad no haya adquirido los derechos correspondientes.

- Transacciones personales:

Los usuarios que utilicen Internet institucional para transacciones personales, como pagos de facturas o operaciones bancarias, asumen los riesgos asociados. La RAP-E Región Central no se responsabiliza por la seguridad de estas transacciones, incluyendo la información transmitida, la cual puede estar sujeta a monitoreo del uso de Internet institucional.

9.1.8 USO DE LA RED INALÁMBRICA

El acceso a la red inalámbrica se proporcionará a dos grupos: invitados y red corporativa. En un evento posterior, se habilitará una zona Wi-Fi gratuita para el público, cumpliendo con lo establecido en el Decreto 728 de 2017 del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). La utilización de los servicios de red estará sujeta a los lineamientos de seguridad aplicables a la red cableada, tal como se detalla en esta política.

El Proceso de Gestión de TICs deberá implementar mecanismos técnicos que aseguren la segmentación de la red inalámbrica, separándola de los demás segmentos de la red cableada institucional. Las redes inalámbricas de invitados y la zona Wi-Fi gratuita no tendrán acceso a los recursos tecnológicos críticos de la LAN, mientras que las áreas autorizadas de la institución podrán acceder a los recursos necesarios para sus operaciones según corresponda.

9.1.9 USO IMPRESIÓN DE INFORMACIÓN CONFIDENCIAL Y POLÍTICA CERO PAPEL

Los colaboradores deberán utilizar la funcionalidad de impresión confidencial en las impresoras institucionales para la impresión de documentos clasificados como confidenciales. Es obligatorio recoger las impresiones inmediatamente después de ser enviadas, con el fin de evitar la pérdida de documentos sensibles o el acceso no autorizado a los mismos.

Asimismo, se prohíbe abandonar documentación en impresoras o escáneres, con el objetivo de proteger la información en formato físico frente a accesos o divulgación no autorizados.

En relación con el envío de correos electrónicos a través de escáneres, se aplican las disposiciones establecidas en este documento para el uso del correo electrónico institucional.

Como parte del compromiso institucional con la Política Cero Papel, se fomentará la adopción de prácticas que prioricen el manejo de documentos en formato digital, contribuyendo a la reducción del consumo de papel y promoviendo la sostenibilidad ambiental.

9.2 CONFIDENCIALIDAD

9.2.1 USO RESPONSABLE DE CONTRASEÑAS

A. Control de Parámetros de Seguridad de las Contraseñas

El Proceso de Gestión de TICs es responsable de implementar y mantener controles que aseguren el uso de parámetros de seguridad robustos para el acceso a los servicios tecnológicos, garantizando así la protección de la información en los sistemas de información y demás componentes tecnológicos de la Entidad.

Para tal fin, se establecen las siguientes medidas:

- **Primer inicio de sesión:** Se solicitará al usuario generar una contraseña propia a partir de la contraseña temporal asignada por defecto.
- **Inactivación de cuentas:** Las cuentas de usuario serán desactivadas automáticamente al vencimiento del contrato laboral o por retiro del colaborador.
- **Lineamientos para la creación de contraseñas:**
    - Longitud mínima de 8 caracteres.
    - Combinación de mayúsculas, minúsculas, letras y números.
    - No incluir espacios en blanco ni secuencias fácilmente predecibles.
- **Autenticación de doble factor (2FA):** Será obligatorio activar un mecanismo de doble factor para el acceso a los servicios tecnológicos institucionales. Este podrá incluir, según la disponibilidad tecnológica, aplicaciones de autenticación, tokens de seguridad, códigos enviados por SMS o correo electrónico, con el fin de fortalecer la protección de las credenciales y reducir el riesgo de accesos no autorizados.

9.3 INTEGRIDAD DE RELACIONAMIENTO INFORMÁTICO

9.3.1 Gestión de Seguridad en Redes

Es fundamental mantener y gestionar adecuadamente las redes para protegerlas frente a amenazas, garantizando la seguridad de los sistemas, aplicaciones y de la información en tránsito. Esta protección se puede lograr mediante la implementación de herramientas como Sistemas de Prevención y/o Detección de Intrusos (IPS/IDS), firewalls, gateways, antivirus, antispam, entre otros.

El acceso a estas herramientas deberá estar estrictamente restringido al personal autorizado del Proceso de Gestión de TICs quien será responsable de su administración y supervisión, garantizando así la integridad y confidencialidad de los recursos tecnológicos de la Entidad.

9.3.2 Redes Contingencias Tecnológicas

Se entiende por contingencia tecnológica cualquier evento que afecte la disponibilidad y prestación de los servicios de tecnologías de la información y las telecomunicaciones, comprometiendo el cumplimiento de los niveles de servicio establecidos con los usuarios. Estos eventos requieren la implementación de soluciones que pueden ir desde alternativas internas de contingencia hasta la activación del Plan de Continuidad del Negocio.

El Proceso de Gestión de TICs deberá implementar configuraciones en alta disponibilidad para reducir la probabilidad de interrupciones en el acceso a la información. Dichas configuraciones deben ser documentadas, probadas y mantenidas por los responsables de la administración de los componentes tecnológicos, asegurando su efectividad frente a posibles contingencias.

9.4 PRUEBAS DE SEGURIDAD DE LA INFORMACIÓN DIGITAL

Se deberán realizar pruebas de seguridad en intervalos planificados, con el objetivo de verificar que los controles y procedimientos cumplen con los requisitos establecidos, evaluando:

- Desempeño: Que los controles funcionen conforme a lo esperado.
- Eficacia: Que los objetivos de seguridad se cumplan de manera efectiva.
- Oportunidades de mejora: Identificación de áreas donde se pueda optimizar la seguridad y la gestión de los controles.

9.5 CLASIFICACIÓN DE LA INFORMACIÓN

La RAP-E Región Central establece un esquema de clasificación de la información, con el fin de garantizar su adecuada gestión, protección y uso:

- **Información Pública:** Aquella cuyo acceso es libre y no requiere autorización, conforme a la Ley 1712 de 2014.
- **Información Interna:** Información de uso exclusivo dentro de la Entidad, cuya divulgación no autorizada puede afectar la operación institucional.

- **Información Confidencial:** Información restringida a funcionarios, contratistas o terceros autorizados, cuya divulgación no autorizada puede generar riesgos legales, financieros o reputacionales.
- **Información Reservada:** Información protegida por mandato legal o decisión administrativa, cuyo acceso está limitado a funcionarios autorizados.
- **Información Sensible:** Datos personales que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación (Ley 1581 de 2012).

Los responsables de cada proceso deberán identificar y clasificar los activos de información bajo su gestión, de acuerdo con estas categorías, y aplicar las medidas de seguridad correspondientes.

9.6 GESTIÓN DE INCIDENTES DE SEGURIDAD DIGITAL

La RAP-E Región Central adoptará un procedimiento para la gestión de incidentes de seguridad de la información que incluya:

- Notificación inmediata de incidentes por parte de los usuarios al Proceso Gestión TICs.
- Registro y trazabilidad de todos los incidentes en un sistema centralizado.
- Clasificación del incidente según su impacto y criticidad.
- Tiempos de respuesta y escalamiento, definidos de acuerdo con los Acuerdos de Niveles de Servicio (ANS).
- Acciones de contención, erradicación y recuperación de la información y servicios afectados.
- Lecciones aprendidas y medidas correctivas/preventivas posteriores al incidente.

El Proceso Gestión TICs será responsable de coordinar la atención de los incidentes y de informar al Comité Institucional de Gestión y Desempeño sobre los eventos críticos.

9.7 PLAN DE CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN ANTE DESASTRES (BCP/DRP)

La RAP-E Región Central definirá y mantendrá actualizado un Plan de Continuidad de Negocio y Recuperación ante Desastres, que contemple:

- Identificación de procesos críticos y dependencias tecnológicas.
- Definición de RPO (Recovery Point Objective) y RTO (Recovery Time Objective).
- Estrategias de respaldo y sitios alternos de operación.
- Pruebas periódicas de restauración de información y servicios.

- Roles y responsabilidades de cada dependencia en caso de contingencia.

El Proceso Gestión TICs será responsable de coordinar la ejecución del plan y asegurar su integración al Sistema Integrado de Gestión (SIG).

9.8 SEGURIDAD EN MOVILIDAD Y TELETRABAJO

En el marco de modalidades de teletrabajo y movilidad, la RAP-E Región Central adoptará medidas de seguridad específicas, tales como:

- Uso obligatorio de VPN institucional para el acceso remoto a los sistemas de información.
- Prohibición de almacenar información sensible en dispositivos personales no autorizados.
- Políticas de uso seguro de Wi-Fi, evitando redes públicas no seguras.
- Reporte inmediato en caso de pérdida o robo de dispositivos.

9.9 GESTIÓN DE PROVEEDORES Y TERCEROS

La RAP-E Región Central establecerá controles para garantizar la seguridad de la información gestionada por terceros, que incluyen:

- Inclusión de cláusulas de confidencialidad, seguridad y protección de datos en todos los contratos.
- Definición de Acuerdos de Niveles de Servicio (ANS/SLA) que incluyan métricas de seguridad y tiempos de respuesta.
- Evaluación periódica de riesgos asociados a proveedores críticos.
- Derecho de la Entidad a realizar auditorías o verificaciones de cumplimiento en materia de seguridad digital.

9.10 MONITOREO DE REGISTROS (LOGS)

La Entidad implementará mecanismos de monitoreo y registro de las actividades en los sistemas de información, con el fin de garantizar la trazabilidad, el no repudio y la protección de los activos tecnológicos. Los registros deberán mantenerse, protegerse y revisarse periódicamente, siguiendo los lineamientos definidos por el Proceso de Gestión TICs.

9.11 SANCIONES POR INCUMPLIMIENTO

El incumplimiento de los lineamientos de la Política de Seguridad de la Información Digital dará lugar a:

- Sanciones disciplinarias para servidores públicos, conforme a la Ley 734 de 2002 – Código Disciplinario Único.
- Sanciones contractuales para contratistas y proveedores, conforme a las cláusulas contractuales y a la Ley 80 de 1993.
- Acciones legales y administrativas que correspondan en caso de afectación grave a la seguridad de la información.

10 INDICADORES DE SEGURIDAD DE INFORMACIÓN DIGITAL

El Proceso de Gestión de TICs deberá identificar, registrar y dar seguimiento a los indicadores de desempeño definidos en la Política de Indicadores de Procesos, disponible en SharePoint.

El seguimiento de estos indicadores permitirá evaluar la efectividad de los procesos, la calidad de los servicios prestados y la oportunidad de mejora continua, asegurando que las operaciones de TIC se alineen con los objetivos institucionales.

Todos los colaboradores responsables del Proceso de Gestión de TICs deberán garantizar el cumplimiento de esta política, utilizando los indicadores como herramienta de control, medición y mejora de los procesos.

FICHA N° 51. INDICADOR: Disponibilidad de Servicios de Conectividad

FICHA DE INDICADOR N° 51	
FACTORES	DESCRIPCIÓN
DEPENDENCIA:	**Dirección Administrativa y Financiera**
NOMBRE DEL INDICADOR:	**Disponibilidad de Servicios de Conectividad**
FAMILIA A LA QUE PERTENECE:	**C-PR.12 Gestión TICs**
FORMULA:	**Cantidad de tiempo sin conectividad**
UNIDAD DE MEDIDA:	**Tiempo Promedio**
CLASIFICACIÓN:	**Gestión**
TIPO DE INDICADOR:	**Eficacia**

SENTIDO O TENDENCIA DEL INDICADOR:	**Positivo**
FRECUENCIA DE MEDICIÓN:	**Semestral**
OPERACIÓN DE CÁLCULO:	**Promediar**
META O TOLERANCIA:	**90% - 100%**
RESPONSABLE DE LA MEDICIÓN:	**Profesional Especializado responsable de Gestión de TICs**
DIMENSIÓN DE MIPG ASOCIADA:	**3. Gestión con Valores para el resultado**
POLÍTICA DE GESTIÓN Y DESEMPEÑO ASOCIADA:	**10. Gobierno digital**

FICHA N° 52. INDICADOR: Seguimiento a la atención de fallas tecnológicas

FICHA DE INDICADOR N° 52	
FACTORES	DESCRIPCIÓN
DEPENDENCIA:	**Dirección Administrativa y Financiera**
NOMBRE DEL INDICADOR:	**Seguimiento a la atención de fallas tecnológicas**
FAMILIA A LA QUE PERTENECE:	**C-PR.12 Gestión TICs**
FORMULA:	**N° Fallas Tecnológicas Atendidas / N° Fallas Tecnológicas Reportadas**
UNIDAD DE MEDIDA:	**Porcentaje**
CLASIFICACIÓN:	**Gestión**

FICHA DE INDICADOR N° 52	
FACTORES	DESCRIPCIÓN
TIPO DE INDICADOR:	**Eficacia**
SENTIDO O TENDENCIA DEL INDICADOR:	**Positivo**
FRECUENCIA DE MEDICIÓN:	**Semestral**
OPERACIÓN DE CÁLCULO:	**Promediar**

META O TOLERANCIA:	**90% - 100%**
RESPONSABLE DE LA MEDICIÓN:	**Profesional Especializado responsable de Gestión de TICs**
DIMENSIÓN DE MIPG ASOCIADA:	**3. Gestión con Valores para el resultado**
POLÍTICA DE GESTIÓN Y DESEMPEÑO ASOCIADA:	**10. Gobierno digital**

FICHA N° 53. INDICADOR: Seguimiento Inventario de licencias instaladas

FICHA DE INDICADOR N° 53	
FACTORES	DESCRIPCIÓN
DEPENDENCIA:	**Dirección Administrativa y Financiera**
NOMBRE DEL INDICADOR:	**Seguimiento Inventario de licencias instaladas**
FAMILIA A LA QUE PERTENECE:	**C-PR.12 Gestión TICs**
FORMULA:	**N° Licencias Registradas en el Inventario / N° Licencias Adquiridas**
UNIDAD DE MEDIDA:	**Porcentaje**
CLASIFICACIÓN:	**Gestión**
TIPO DE INDICADOR:	**Eficacia**
SENTIDO O TENDENCIA DEL INDICADOR:	**Positivo**
FRECUENCIA DE MEDICIÓN:	**Semestral**
OPERACIÓN DE CÁLCULO:	**Promediar**
META O TOLERANCIA:	**90% - 100%**
RESPONSABLE DE LA MEDICIÓN:	**Profesional Especializado responsable de Gestión de TICs**
DIMENSIÓN DE MIPG ASOCIADA:	**3. Gestión con Valores para el resultado**
POLÍTICA DE GESTIÓN Y DESEMPEÑO ASOCIADA:	**11. Seguridad digital**

FICHA N° 54. INDICADOR: Seguimiento al cumplimiento de los ANS

FICHA DE INDICADOR N° 54	
FACTORES	DESCRIPCIÓN
DEPENDENCIA:	**Dirección Administrativa y Financiera**
NOMBRE DEL INDICADOR:	**Seguimiento al cumplimiento de los ANS**
FAMILIA A LA QUE PERTENECE:	**C-PR.12 Gestión TICs**
FORMULA:	**Cantidad de tiempo de atención en las Fallas Tecnológicas Atendidas por Terceros**
UNIDAD DE MEDIDA:	**Tiempo Promedio**

CLASIFICACIÓN:	**Gestión**
TIPO DE INDICADOR:	**Eficacia**
SENTIDO O TENDENCIA DEL INDICADOR:	**Positivo**
FRECUENCIA DE MEDICIÓN:	**Semestral**
OPERACIÓN DE CÁLCULO:	**Promediar**
META O TOLERANCIA:	**90% - 100%**
RESPONSABLE DE LA MEDICIÓN:	**Profesional Especializado responsable de Gestión de TICs**
DIMENSIÓN DE MIPG ASOCIADA:	**3. Gestión con Valores para el resultado**
POLÍTICA DE GESTIÓN Y DESEMPEÑO ASOCIADA:	**11. Seguridad digital**

FICHA N° 55. INDICADOR: Mantenimiento correctivo de hardware y software

FICHA DE INDICADOR N° 55	
FACTORES	DESCRIPCIÓN
DEPENDENCIA:	**Dirección Administrativa y Financiera**
NOMBRE DEL INDICADOR:	**Mantenimiento correctivo de hardware y software**
FAMILIA A LA QUE PERTENECE:	**C-PR.12 Gestión TICs**
FORMULA:	**N° Mantenimientos Realizados / N° Mantenimientos Programados**
UNIDAD DE MEDIDA:	**Porcentaje**
CLASIFICACIÓN:	**Gestión**
TIPO DE INDICADOR:	**Eficacia**
SENTIDO O TENDENCIA DEL INDICADOR:	**Positivo**
FRECUENCIA DE MEDICIÓN:	**Semestral**
OPERACIÓN DE CÁLCULO:	**Promediar**
META O TOLERANCIA:	**90% - 100%**
RESPONSABLE DE LA MEDICIÓN:	**Profesional Especializado responsable de Gestión de TICs**
DIMENSIÓN DE MIPG ASOCIADA:	**3. Gestión con Valores para el resultado**
POLÍTICA DE GESTIÓN Y DESEMPEÑO ASOCIADA:	**11. Seguridad digital**

FICHA N° 56. INDICADOR: Copias de Seguridad

FICHA DE INDICADOR N° 56	
FACTORES	DESCRIPCIÓN
DEPENDENCIA:	**Dirección Administrativa y Financiera**
NOMBRE DEL INDICADOR:	**Copias de Seguridad**
FAMILIA A LA QUE PERTENECE:	**C-PR.12 Gestión TICs**

FORMULA:	**N° Copias de Seguridad Realizadas / N° Copias de Seguridad Programadas**
UNIDAD DE MEDIDA:	**Cantidad**
CLASIFICACIÓN:	**Gestión**
TIPO DE INDICADOR:	**Eficacia**
SENTIDO O TENDENCIA DEL INDICADOR:	**Positivo**
FRECUENCIA DE MEDICIÓN:	**Semestral**
OPERACIÓN DE CÁLCULO:	**Promediar**
META O TOLERANCIA:	**90% - 100%**
RESPONSABLE DE LA MEDICIÓN:	**Profesional Especializado responsable de Gestión de TICs**
DIMENSIÓN DE MIPG ASOCIADA:	**3. Gestión con Valores para el resultado**
POLÍTICA DE GESTIÓN Y DESEMPEÑO ASOCIADA:	**11. Seguridad digital**

11 GLOSARIO

- **Activo de Información:** Recurso humano, físico o tecnológico con valor para la Entidad que administra, contiene, procesa o transmite información mediante medios físicos, electrónicos, magnéticos u ópticos. [Definición adaptada de ISO/IEC 27001:2013].

- **Componente Tecnológico:** Elemento que facilita servicios de procesamiento, transmisión o almacenamiento de información.
- **Infraestructura Tecnológica:** Conjunto de hardware, software y servicios de telecomunicaciones que soportan la operación del área TIC.
- **Hardware:** Partes físicas y tangibles de un sistema tecnológico.
- **Software:** Conjunto de componentes lógicos que permiten realizar tareas específicas.
- **Software de Dominio Público:** Software de libre uso, sin derechos de autor, que puede incorporarse a desarrollos no comerciales.
- **Software Ilegal:** Uso o copia no autorizada de un programa fuera de lo permitido por la ley o licencia. [Ley 603 de 2000 – Derecho de autor].
- **Confidencialidad:** Prevención del acceso o divulgación de información a personas no autorizadas. [NTC-ISO/IEC 27001:2013].
- **Disponibilidad:** Condición de la información de estar accesible a personas, procesos o aplicaciones autorizadas cuando lo requieran. [NTC-ISO/IEC 27001:2013].
- **Integridad:** Salvaguarda de la exactitud y completitud de la información y sus métodos de procesamiento. [NTC-ISO/IEC 27001:2013].
- **Autenticidad:** Garantía de validez y origen de la información, evitando suplantaciones. [ISO/IEC 27002:2022].
- **No Repudio:** Garantía de que el emisor o receptor de un mensaje no pueda negar su participación. [ISO/IEC 27001:2013].
- **Dato Personal:** Información asociable a una persona natural determinada o determinable. [Ley 1581 de 2012 – Art. 3].
- **Datos Sensibles:** Información que afecta la intimidad del titular o puede generar discriminación. [Ley 1581 de 2012 – Art. 4].
- **Dato Público:** Información no semiprivada, privada o sensible, presente en registros o documentos públicos. [Ley 1581 de 2012].
- **Dato Semiprivado:** Información que no es íntima ni pública, pero puede interesar a sectores específicos, como datos financieros o crediticios. [Ley 1266 de 2008].
- **Dato Privado:** Información de naturaleza íntima o reservada relevante únicamente para el titular. [Ley 1581 de 2012].

- **Derecho de Habeas Data:** Derecho a conocer, actualizar y rectificar la información recogida sobre una persona en bases de datos y archivos. [Art. 15, Constitución Colombiana].
- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información, incluyendo autenticidad, responsabilidad, no repudio y confiabilidad. [NTC-ISO/IEC 27001:2013].
- **Evento de Seguridad de la Información:** Condición que indica posibles violaciones a la política de seguridad o fallas de salvaguardas. [NTC-ISO/IEC 27001:2013].
- **Emergencia Tecnológica:** Evento que interrumpe servicios tecnológicos, causando indisponibilidad de información.
- **Firewall:** Sistema que separa redes, asegurando que las comunicaciones cumplan políticas de seguridad.
- **Antivirus:** Software que detecta, limpia y/o elimina virus informáticos. [ISO/IEC 27002:2022].
- **Antispam:** Mecanismo que previene la recepción de correos no deseados. [ISO/IEC 27002:2022].
- **Código Malicioso:** Programa con fines maliciosos (virus, scripts, macros) que puede propagarse, robar información o controlar equipos.
- **Firma Digital:** Código electrónico que autentica la identidad del emisor de un mensaje o documento.
- **Autorización:** Consentimiento expreso e informado del titular para el tratamiento de sus datos.
- **Aviso de Privacidad:** Comunicación que informa al titular sobre las políticas y finalidades del tratamiento de sus datos. [Ley 1581 de 2012].

12 DIFUSIÓN DE LA POLÍTICA

La presente Política de Seguridad de la Información Digital será difundida de manera oportuna y accesible a todos los funcionarios, contratistas y terceros que tengan relación con la Entidad, garantizando su conocimiento y aplicación en el ejercicio de sus funciones y actividades.

La Entidad dispondrá de mecanismos de divulgación tales como:

- Publicación en la página web institucional, en cumplimiento de la Ley 1712 de 2014 –Ley de Transparencia y Acceso a la Información Pública–.
- Correos electrónicos y medios institucionales de comunicación.
- Inclusión en procesos de inducción y reinducción de funcionarios y contratistas.
- Capacitaciones periódicas orientadas a reforzar las responsabilidades frente a la seguridad de la información.

Será responsabilidad de las dependencias competentes de la Entidad velar por la actualización, divulgación y comprensión de esta Política, así como de los lineamientos, manuales y normas asociadas, garantizando que todos los actores involucrados conozcan y cumplan las disposiciones aquí establecidas.

13 AUDITORÍA Y REVISIÓN

La responsabilidad del seguimiento y verificación del cumplimiento de la presente Política de Seguridad de la Información Digital estará a cargo de la oficina de Control Interno de la entidad, el cual realizará la auditoría de manera anual, con el fin de evaluar la efectividad de los controles y garantizar la mejora continua.

El proceso de Gestión TICs será responsable de la revisión y actualización de la presente Política, la cual deberá realizarse como mínimo cada dos (2) años, o antes si se presentan cambios normativos, tecnológicos o de gestión que lo requieran.

14 CONTROL DE CAMBIOS

VERSIÓN	FECHA	PROCESO	DESCRIPCIÓN
V.1	Noviembre 2025	Gestión TICs	Versión inicial
V.2	Enero 2026	Gestión TICs	Actualización de los lineamientos sobre Tratamiento de Datos Personales, uso de WhatsApp Institucional, publicación de documentos en la página web institucional y responsabilidades del usuario en el correo institucional.