
 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 1 de 41

TABLA DE CONTENIDO

INTRODUCCIÓN.....	3
1. OBJETIVO.....	3
2. ALCANCE.....	3
3. DEFINICIONES.....	3
4. MARCO NORMATIVO.....	8
5. DESARROLLO.....	11
5.1. PRINCIPIOS DE TI.....	11
5.2. POLÍTICAS GENERALES DE TI.....	12
5.2.1. Políticas generales de alineación de TI con los objetivos estratégicos.....	14
5.2.2. Políticas generales de uso eficiente de los recursos de TI.....	16
5.2.3. Políticas generales de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación, Políticas generales de manejo de información.....	19
5.2.4. Políticas generales de gobierno de datos e información.....	23
5.2.5. Políticas generales el dato público es compartido.....	26
5.2.6. Políticas generales de accesibilidad de datos.....	28
5.2.7. Políticas generales de calidad de los datos y la información.....	30
5.2.8. Políticas generales de interoperabilidad y colaboración.....	33
5.2.9. Políticas generales de servicios compartidos de infraestructura de TI.....	36
5.2.10. Políticas generales de disponibilidad de la infraestructura de TI.....	38
5.2.11. Políticas generales de uso y apropiación de TI.....	39
6. CONTROL DE CAMBIOS.....	41


¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 2 de 41

ÍNDICE DE TABLAS

Tabla 1 Políticas generales de TI	12
Tabla 3 Listado de políticas de alineación TI con los objetivos estratégicos	14
Tabla 4 Políticas específicas de alineación de TI con los objetivos estratégicos	16
Tabla 5 Listado de políticas de uso eficiente de los recursos de TI.....	17
Tabla 6 Políticas específicas del uso eficiente de los recursos de TI	18
Tabla 7 Listado de políticas de seguridad de la información	19
Tabla 8 Políticas específicas de seguridad de la información	20
Tabla 9 Listado de políticas de gobierno de datos e información	23
Tabla 10 Políticas específicas de gobierno de datos e información	25
Tabla 11 Listado políticas de dato público compartido	26
Tabla 12 Políticas específicas de dato público compartido	27
Tabla 13 Listado de políticas de accesibilidad de datos.....	28
Tabla 14 Políticas específicas relacionadas con la accesibilidad de datos	29
Tabla 15 Listado de políticas de calidad de los datos y la información	30
Tabla 16 Políticas específicas de calidad de los datos y la información.....	31
Tabla 17 Listado de políticas de interoperabilidad y colaboración	33
Tabla 18 Políticas específicas relacionadas con la interoperabilidad y colaboración	34
Tabla 19 Listado de políticas de servicios compartidos de infraestructura de TI.....	36
Tabla 20 Políticas específicas de los servicios compartidos de infraestructura de TI	37
Tabla 21 Listado de políticas de disponibilidad de la infraestructura de TI.....	38
Tabla 22 Políticas específicas de disponibilidad de la infraestructura de TI.....	39
Tabla 23 Listado de políticas de uso y apropiación de TI.....	40
Tabla 24 Políticas específicas de uso y apropiación de TI	40
Tabla 25 Control de cambios.....	41

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 3 de 41

INTRODUCCIÓN

El ICBF pertenece al sector de la inclusión social y la reconciliación, cuyo propósito sectorial es *“Construir grandes historias de inclusión social y reconciliación para Colombia”*.

La Entidad cabeza de sector es Prosperidad Social, quien formuló en el año 2017, la *“Guía de Principios y Políticas Generales de TIC: para Prosperidad Social y el Sector”*, para fortalecer las políticas y lineamientos de TI para el sector de la inclusión social y la reconciliación.

El ICBF, por su parte, en cabeza de la Dirección de Información y Tecnología, ha consolidado políticas de TI, de acuerdo con el esquema metodológico planteado en el modelo de gestión estratégica de TI (IT4+), no obstante, se ha identificado brechas en esta alineación por lo cual, siguiendo los lineamientos de la Guía formulada por Prosperidad Social para el Sector, se establece la presente Guía para el ICBF.

1. OBJETIVO

Definir, los principios y políticas generales de TIC basadas en el Marco de Referencia de Arquitectura Empresarial de Tecnologías de la Información Colombia, para aplicarlas según corresponda y sea pertinente.

2. ALCANCE

El presente documento debe ser aplicado en el marco de los diferentes procesos, por los, servidores públicos y contratistas del ICBF en cada una de las dependencias, así como, proveedores y operadores de servicios del Instituto en la sede de la dirección general, regionales y centros zonales.


3. DEFINICIONES

- **Accesibilidad:** es una característica deseable en las páginas web e interfaces gráficas de los sistemas de información que consiste en la posibilidad que tiene un usuario de acceder a un sitio web y navegar en él, sin importar que cuente con algún tipo de discapacidad.¹
- **Activo de Información:** se denomina activo a aquello que tiene valor para la organización y por lo tanto debe protegerse. De manera que un activo de información es aquel que contiene o manipula información, abarcando seguridad digital y continuidad de la operación².

¹ Ministerio TIC, *“Manual de Gobierno Digital” disponible digital en la página de gobierno digital.*

² *“Guía para el Desarrollo de Inventario y Clasificación de Activos G10.GTI”* Disponible digital en la página web del ICBF.

¡Antes de imprimir este documento... piense en el medio ambiente!


 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 4 de 41

- **Servicios de TI:** conjunto de actividades que buscan responder a las necesidades de un cliente por medio de un cambio de condición en los bienes informáticos.
- **Análisis de riesgos:** uso sistemático de una metodología para estimar los riesgos e identificar sus fuentes, para los activos o bienes de información.
- **ANS (Acuerdos de Niveles de Servicios):** indicadores basados en métricas que determinan la cabalidad en el cumplimiento de la entrega o prestación de un servicio de TI.
- **Atributo de calidad:** condiciones o cualidades calificables (cualitativa o cualitativamente) y que indican el estado de una unidad de información, respecto de unos parámetros definidos.
- **Autenticidad:** propiedad que garantiza que la identidad de un sujeto o recurso es la que se declara. La autenticidad se aplica a entidades como a usuarios, procesos, sistemas e información.
- **Clasificación de la Información:** es el ejercicio por medio del cual se determina el nivel de protección de la información producto de la operación del ICBF, definidas en el inventario de activos de información; su clasificación tiene como objetivo asegurar que la información tenga el nivel de protección adecuado.³
- **Colaborador:** toda persona que tenga vínculo laboral como servidor público o contrato por prestación de servicio con el ICBF.
- **Confiabilidad:** propiedad de tener comportamiento y resultados previstos consistentes.
- **Control:** una forma para manejar el riesgo, incluyendo políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas, y que pueden ser de carácter administrativo, técnico o legal.
- **Creación de valor:** las TIC crean valor, cuando son capaces de ofrecer mejores características de desempeño, en la operación y /o gestión de los procesos misionales o de soporte, comparados en referencia a la forma tradicional de su ejecución. La estrategia es una de las primeras formas para crear valor. Por otro lado, según el Manual de Gobierno Digital, el valor público es el fin último del uso de la tecnología en la relación del Estado, ciudadanos, usuarios y grupos de interés. El valor público se relaciona con el desarrollo social, la gobernanza, la garantía de derechos, la satisfacción de necesidades, la prestación de servicios de calidad y el mejoramiento de las condiciones de vida de la sociedad. No sólo es hacer uso de las tecnologías, sino cómo las tecnologías ayudan a resolver problemas reales. Valor público también es lograr que el Estado llegue a donde no llega el mercado, satisfaciendo necesidades y problemáticas.
- **Dato:** es la representación simbólica, característica o atributo de un objeto o entidad.
- **Datos abiertos:** la Carta Internacional de Datos Abiertos define los datos abiertos como *“datos digitales que son puestos a disposición con las características técnicas y jurídicas necesarias para que puedan ser usados, reutilizados y redistribuidos libremente por cualquier persona, en cualquier momento y en cualquier lugar”*.⁴ A partir de ello, los datos abiertos son considerados como uno de los factores que impulsan la transformación

³ “GUÍA PARA LA ROTULACIÓN DE LA INFORMACIÓN” Disponible digital en la página web del ICBF.

⁴ Tomado de “ABC de Datos Abiertos, qué son y por qué usarlos” sitio web metropol.

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 5 de 41

global favorecida por la tecnología y los medios digitales y permiten a los gobiernos, ciudadanos y organizaciones de la sociedad civil y del sector privado tomar mejores decisiones informadas.


- **Datos Analíticos:** son datos que ayudan y posibilitan la toma de decisiones, y están orientados a un determinado ámbito dentro de la organización.
- **Datos maestros:** datos que son compartidos por varios procesos y deben ser tratados como un activo estratégico.
- **Datos Operacionales:** son datos utilizados en el día a día de la entidad, sustentan la operación institucional y por lo tanto son datos activos (están en variación constante).
- **Diccionario de Datos:** conjunto de términos y sus definiciones, asociados a un modelo de datos; el diccionario de datos contiene la definición semántica de un campo en una estructura de datos.
- **Eco – eficiente:** está basado en el concepto de crear más bienes y servicios utilizando menos recursos y creando menos basura y polución.
- **Estandarización:** modelo o patrón que permite la unificación de tecnologías con finalidades distintas.
- **Estrategia:** es un conjunto de compromisos y acciones, integrados y coordinados, diseñados para explotar las competencias centrales y lograr una ventaja competitiva.
- **Incidente de seguridad de la información:** evento o serie de eventos de seguridad de la información (cualquier situación identificada que indique una posible brecha en las políticas de seguridad o falla en los controles y/o protecciones establecidas) no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información ⁵.
- **Índice de calidad de la información:** métrica utilizada para determinar la variación en la calidad de las unidades de información de un proceso de negocio; su medición es porcentual.
- **Información:** datos relacionados que tienen significado para la entidad. La información es un activo que, como otros activos importantes, es esencial para las actividades estratégicas y misionales y, en consecuencia, necesita una protección adecuada. La información se valora como un bien público.⁶
- **Información pública:** toda la información que el Instituto Colombiano de Bienestar Familiar (ICBF), genere, obtenga, o controle, la cual puede ser entregada y/o publicada sin restricciones a terceros, colaboradores o cualquier persona sin representar riesgo para los procesos del ICBF.⁷
- **Información clasificada:** aquella información que estando en poder o custodia del Instituto Colombiano de Bienestar Familiar (ICBF), pertenece al espacio propio, particular y privado o semiprivado de una persona natural o jurídica, por lo cual su acceso podrá

⁵ Norma Técnica ISO/IEC 27001:2013

⁶ Tomado de "ABC de Datos Abiertos, qué son y por qué usarlos" sitio web metropol.

⁷ Ley 1712 de 2012

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 6 de 41

ser negado o exceptuado al público.⁸ (Tomado de la Ley 1712 de 2014, de acuerdo con la operación del ICBF).

- **Información reservada:** es aquella información que estando en poder o custodia del Instituto Colombiano de Bienestar Familiar (ICBF), sea negado su acceso al público por daño a intereses públicos, porque excluye algunos temas que se salen del término seguridad pública, ejemplo salud pública, etc.
- **Información no estructurada:** información que no tiene estructura de datos, no cuenta con un esquema particular o una estandarización ideada y definida.
- **Infraestructura de TI:** se refiere a la plataforma tecnológica que permite la prestación de servicios de TI.
- **Integridad:** propiedad de salvaguarda la exactitud y estado completo de los activos, busca mantener los datos libres de modificaciones no autorizadas.
- **Mapa de información:** representación gráfica de las unidades de información, debe tener en cuenta los atributos de calidad definidos y su valoración. También se describe como un proceso de mejora de la definición y del intercambio de flujos relevantes de las instituciones, desde la perspectiva del uso y valor de la información.
- **Marco de Interoperabilidad:** conjunto de elementos que orientan el intercambio de información a nivel público y está constituido por: principios, políticas, un modelo de administración, un modelo de madurez, un modelo de medición, un conjunto de recomendaciones, protocolos, estándares y guías metodológicas.⁹
- **Medios de acceso:** son formas existentes que permiten el acceso.
- **Metadatos:** información necesaria para el uso e interpretación de los datos. Los metadatos describen la conceptualización, calidad, generación, cálculo y características de un conjunto de datos.
- **Plan:** iniciativas encaminadas a suplir necesidades identificadas.
- **Plan estratégico de TI:** de acuerdo con el Marco de Referencia de Arquitectura Empresarial para la Gestión de TI del Estado colombiano, el Plan Estratégico de las Tecnologías de la Información (PETI) o también conocido como Planes estratégicos de las Tecnologías de la información y las Comunicaciones (PETIC) *“es el artefacto que se utiliza para expresar la Estrategia de TI. El PETI hace parte integral de la estrategia de la institución y es el resultado de un adecuado ejercicio de planeación estratégica de TI.”*¹⁰ Cada vez que una institución pública hace un ejercicio o proyecto de Arquitectura Empresarial, su resultado debe ser integrado al PETI.
- **Plataforma de Interoperabilidad:** es el conjunto de herramientas necesarias para que los sistemas de información del Estado conversen entre sí. Integra los diferentes servicios y trámites prestados por el Estado.¹¹
- **Probidad:** oralidad, integridad y honradez en las acciones.


⁸ Ídem anterior

⁹ MinTIC “Marco de interoperabilidad” disponible en línea.

¹⁰ MinTIC “Guía Cómo Estructurar el Plan Estratégico de Tecnologías de la Información - PETI”

¹¹ MinTIC “Marco de interoperabilidad” disponible en línea.

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 7 de 41

- **Proyecto:** “Es un esfuerzo temporal que se lleva a cabo para crear, un producto, servicio o resultado único”¹². Cuenta con un claro patrocinador y con su aprobación.
- **Resiliencia:** capacidad para reponerse y superar eventos adversos.
- **Reglas de validación:** los pasos o validaciones que han de ejecutarse para determinar que una unidad de información cumple con los criterios mínimos especificados en un determinado atributo de calidad.
- **Reglas de corrección:** los pasos que han de ejecutarse para corregir una unidad de información de acuerdo con los criterios mínimos especificados en un determinado atributo de calidad.
- **Riesgo – cumplimiento:** es la interrelación que permite maximizar el valor de las oportunidades y optimizar su rendimiento a través de la gestión del Riesgo y la Incertidumbre, mientras se mantienen dentro de los límites del cumplimiento con las obligaciones legales.
- **Seguridad informática:** protección de la infraestructura computacional y todo lo relacionado con esta, incluyendo la información contenida.
- **Dominio semántico de interoperabilidad:** permite garantizar que, en el momento de intercambiar datos, el significado de la información sea el mismo para todos los actores involucrados.¹³
- **Servicio de intercambio de información:** mecanismo para intercambiar información a través de un medio de transmisión electrónico, magnético o telemático.¹⁴
- **Tecnología verde:** se refiere al uso eficiente de los recursos computacionales minimizando el impacto ambiental, maximizando su viabilidad económica y asegurando deberes sociales.
- **Terceras partes:** se entiende por tercero a toda persona, jurídica o natural, como proveedores, contratistas o consultores, que provean servicios o productos a la Entidad.
- **Tecnología de la Información (TI):** abarca el dominio completo de la información, que incluye al hardware, al software, a los periféricos y a las redes.¹⁵
- **Tecnologías de la Información y las Comunicaciones (TIC):** son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes.¹⁶
- **Unidad de Información:** pieza crítica y relevante de información que es necesaria para realizar o ejecutar un proceso misional. Sobre ella se fundamentan las decisiones.
- **Valoración cualitativa:** valoración de alto nivel basada en la percepción sobre los atributos de calidad y dada por los dueños de las unidades de información.

¹² Way Back Machine “Proyectos” disponible en línea


¹³ Ídem anterior

¹⁴ MinTIC “Marco de interoperabilidad” disponible en línea

¹⁵ EHOW “TI” disponible digital

¹⁶ MinTIC “TIC” disponible en línea

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 8 de 41


- **Valoración cuantitativa:** valoración de los atributos de calidad de la información realizada con herramientas informáticas y aplicadas sobre información almacenada en bases de datos.
- **W3C:** World Wide Web Consortium, comunidad internacional que desarrolla estándares para el crecimiento de la web.

4. MARCO NORMATIVO

El marco normativo que aplica para la gestión de TI en el Estado colombiano es bastante amplio, a continuación, se señalan los más relevantes:


- **Ley 1955 de 2019:** por el cual se expide el Plan Nacional de Desarrollo 2018 - 2022 "Pacto por Colombia, pacto por la equidad".
- **Ley 1978 de 2019:** por la cual se moderniza el sector de las tecnologías de la información y las comunicaciones -tic, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones.
- **Ley 23 de 1982:** sobre derechos de autor.
- **Ley 1915 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.
- **Ley 1712 de 2014:** "*Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones*".
- **Decreto 1081 de 2015,** "*Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones*", el cual facilita la implementación y cumplimiento de la Ley 1712 en los temas relacionados con la gestión de la información pública en cuanto a su adecuada publicación y divulgación, la recepción y respuesta a solicitudes de acceso a ésta, su adecuada clasificación y reserva, la elaboración de los instrumentos de gestión de información, así como el seguimiento de la misma; y la resolución 3564 de 2015 del Ministerio de Tecnologías de la Información y las Comunicaciones, "*Por la cual se reglamentan aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública*", que tiene por objeto establecer lineamientos respecto de los estándares y divulgación de la información, accesibilidad en medio electrónicos para población en situación de discapacidad, formulario electrónico para la recepción de solicitudes de acceso a información pública, condiciones técnicas para la publicación de datos abiertos y condiciones de seguridad de los medios electrónicos.
- **Decreto 1078 de 2015:** específicamente en su título 9 políticas y lineamientos de tecnologías de la información, capítulo 1. Estrategia de Gobierno en Línea, cuyo objeto es "*Definir los lineamientos, instrumentos y plazos de la estrategia de Gobierno en Línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado abierto, más eficiente, más transparente y participativo y que preste mejores servicios con la colaboración de toda la sociedad*".

¡Antes de imprimir este documento... piense en el medio ambiente!

	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 9 de 41

- **Decreto 415 de 2016:** *"Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones."* El cual establece los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones - TIC a través del posicionamiento de los líderes de áreas TI y la definición de objetivo para el fortalecimiento institucional.
- **Ley 1581 de 2012:** por la cual se dictan disposiciones generales para la protección de datos personales.
- **Ley 1437 de 2011:** por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- **Ley 1273 de 2009:** por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado *"de la protección de la información y de los datos"* y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **Ley 1266 de 2008:** por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- **Ley 594 de 2000:** por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
- **Ley 1341 de 2009:** *"Artículo 2.2.9.1.1.3. Principios. La Política de Gobierno Digital se desarrollará conforme a los principios que rigen la función y los procedimientos administrativos consagrados en los artículos 209 de la Constitución Política, 3° de la Ley 489 de 1998, 3° de la Ley 1437 de 2011, 2 Y 3 de la Ley 1712 de 2014, así como los que orientan el sector TIC establecidos en el artículo 2 de la Ley 1341 de 2009, y en particular los siguientes:*
 - *Innovación: en virtud de este principio el Estado y los ciudadanos deben propender por la generación de valor público a través de la introducción de soluciones novedosas que hagan uso de TIC, para resolver problemáticas o necesidades identificadas.*
 - *Competitividad: según este principio el Estado y los ciudadanos deben contar con capacidades y cualidades idóneas para actuar de manera ágil y coordinada, optimizar la gestión pública y permitir la comunicación permanente a través del uso y aprovechamiento de las TIC.*
 - *Proactividad: con este principio se busca que el Estado y los ciudadanos trabajen de manera conjunta en el diseño de políticas, normas, proyectos y servicios, para tomar decisiones informadas que se anticipen a los acontecimientos, mitiguen riesgos y atiendan a las necesidades específicas de los usuarios, buscando el restablecimiento de los lazos de confianza a través del uso y aprovechamiento de las TIC.*
 - *Seguridad de la Información: este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos,*


¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 10 de 41

preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.”

- **Decreto 1377 de 2013:** por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015.
- **Decreto 3816 de 2003:** por el cual se crea la Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública.
- **Decreto 1008 de 2018:** *"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".*
- **Decreto 019 de 2012:** por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
- **Decreto 2609 de 2012:** por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- **Decreto 0988 de 2012:** por el cual se aprueba la modificación de la planta de personal del Instituto Colombiano de Bienestar Familiar *"Cecilia de la Fuente de Lleras"* y se dictan otras disposiciones.
- **Decreto 1413 de 2017:** por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título 111 de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- **Decreto 1081 de 2015:** por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República.
- **Decreto 0987 de 2012:** por el cual se modifica la estructura del Instituto Colombiano de Bienestar Familiar *"Cecilia de la Fuente de Lleras"* y se determinan las funciones de sus dependencias.
- **Decreto 235 de 2010:** por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones.
- **Decreto 612 de 2018:** por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- **Decreto 3816 de 2003:** *"Por el cual se crea la Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública".*
- **Decreto 620 de 2020:** *"Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60. 61 Y 64 Ley 1437 de 2011. los literales e, j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del*

iAntes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 11 de 41

Decreto 2106 de 2019. estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales"

Cabe precisar que en el marco de la implementación de los Sistema Integrado de Gestión - SIGE, ISO/ IEC 27001:2013, ISO 9001:2015, ISO 14001:2015 e ISO 45001:2018, el ICBF cuenta con Matrices de Requisitos Legales para estos cuatro ejes, como un mecanismo de verificación de cumplimiento de las normas aplicables, matrices publicadas en la Intranet del ICBF y de forma complementaria el Anexo No. 1. Marco Normativo, que hace parte del PETI.

5. DESARROLLO


En este capítulo se relacionan los principios y políticas de TI que rigen para el Instituto Colombiano de Bienestar Familiar – ICBF, que toma como referencia los definidos por Prosperidad Social como cabeza del sector de Inclusión y Reconciliación.

5.1. PRINCIPIOS DE TI

A continuación, se detallan los principios de TI para el ICBF, base fundamental para las políticas generales de TI.

- a. **El dato es un activo y se gobierna:** los datos del ICBF son activos intangibles de muy alto valor y como tal se les debe proveer el tratamiento correspondiente a la recolección, uso, gestión y suministro preciso y oportuno de los mismos.
- b. **El dato público es compartido:** los datos del ICBF que estén clasificados como públicos, deben ser compartidos para lograr mayor eficiencia en los procesos como muestra de transparencia y de buen gobierno.
- c. **El dato es accesible:** los datos del ICBF se deben encontrar a disposición de quienes requieran acceder a ellos, grupos de interés, procesos o aplicaciones.
- d. **Calidad de los datos:** los datos deben ser completos, exactos, responder con veracidad a la situación actual del ICBF, ser aptos para su uso y cumplir con el conjunto de atributos relevantes de calidad de datos definido.
- e. **Seguridad de la información:** la información debe ser clasificada y protegida contra la divulgación y uso no autorizado.
- f. **Alineación de TI con los objetivos estratégicos:** los planes y proyectos en tecnologías de la información y las comunicaciones deben estar orientados al cumplimiento de la misión, los objetivos estratégicos del ICBF y satisfacer las necesidades derivadas de la estrategia misional.
- g. **Interoperabilidad y colaboración:** los procesos del ICBF deben compartir datos y posibilitar el intercambio de información entre ellos, con otras entidades y con el ciudadano. La interoperabilidad es necesaria y prioritaria para la cooperación, desarrollo, integración y prestación del servicio a nuestros beneficiarios, mejorar los procesos internos y dar cumplimiento a la Ley.

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 12 de 41

- h. **Uso eficiente de los recursos de TI:** el ICBF debe establecer mecanismos para el uso eficiente de los recursos de tecnología. Las adquisiciones se deben hacer en razón a la priorización de necesidades, con base en análisis adecuados y permanentes. Las TI deben estar dimensionadas para dar soporte a la organización, proporcionando servicios con calidad.
- i. **Servicios compartidos de infraestructura:** el ICBF debe centralizar las actividades comunes, economizando en recursos humanos, infraestructura, incrementando el mejoramiento del servicio, así mismo contar con una infraestructura tecnológica centralizada, estandarizada y dimensionada para dar soporte a toda la entidad.
- j. **Disponibilidad de la infraestructura de TI:** la infraestructura de hardware, software y telecomunicaciones debe estar en funcionamiento y al servicio de los usuarios internos y externos cuando lo requieran.
- k. **Uso y apropiación de soluciones TI:** las iniciativas de TI deben contar con estrategias de uso y apropiación que promuevan las buenas prácticas para el correcto uso y aprovechamiento de las soluciones de TI que aportan a los procesos del ICBF.

5.2. POLÍTICAS GENERALES DE TI


En esta sección se detallan las Políticas Generales de TI del ICBF, teniendo en cuenta los lineamientos definidos por Prosperidad Social para las entidades adscritas a este sector.

En la tabla que se presenta a continuación, se muestra la relación existente entre los dominios del Marco de Referencia de Arquitectura Empresarial, los principios anteriormente mencionados y las políticas de TI que se describen con detalle en este capítulo.

Tabla 1 Políticas generales de TI


DOMINIO DE ARQUITECTURA	PRINCIPIOS GENERALES DE TI	POLÍTICAS GENERALES	POLÍTICAS ESPECIFICAS
<ul style="list-style-type: none"> • Estrategia TI • Gobierno TI 	Alineación de TI con los objetivos estratégicos	Alineación de TI con los objetivos estratégicos	1. Plan Estratégico de Tecnología 2. Coherencia con los proyectos de inversión pública nacional 3. Interacción entre TI y las dependencias 4. Gobierno de TI 5. Administración del portafolio de proyectos de TI 6. Alineación entre los sistemas de información y los procesos
<ul style="list-style-type: none"> • Estrategia TI • Gobierno TI 	Uso eficiente de los recursos de TI	Uso eficiente de los recursos de TI	1. Estandarización 2. Capacidad de la infraestructura 3. Mantener lo simple y funcional 4. Tecnología verde 5. Procesos internos Contratación
<ul style="list-style-type: none"> • Gobierno TI de Información 	Seguridad de la información	Seguridad y Privacidad de la información	1. Estandarización 2. Gestión de Activos 3. Control de Acceso

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 13 de 41

DOMINIO DE ARQUITECTURA	PRINCIPIOS GENERALES DE TI	POLÍTICAS GENERALES	POLÍTICAS ESPECÍFICAS
<ul style="list-style-type: none"> • Sistemas Información • Servicios Tecnológicos 		Seguridad Digital Continuidad de la Operación	4. Criptografía 5. Seguridad Física y del Entorno 6. Seguridad de las Operaciones 7. Seguridad de las Comunicaciones 8. Seguridad para la Adquisición, Desarrollo y Mantenimiento de Sistemas 9. Seguridad para Relación con los Proveedores 10. Gestión de Incidentes de Seguridad de la Información 11. Continuidad de la Operación Cumplimiento
<ul style="list-style-type: none"> • Información 	El dato es un activo y se gobierna	Gobierno de datos e información	1. Gobierno de los datos 2. Responsabilidad compartida 3. Toma de consciencia 4. Organización del gobierno de datos 5. Identificación y caracterización de datos 6. Auditoría, medición y mejora 7. Decisiones basadas en Información
<ul style="list-style-type: none"> • Información 	El dato público es compartido	El dato público es compartido	1. Concordancia con las Políticas de Seguridad de la Información 2. Apertura de datos 3. Divulgación activa de la información pública 4. Sensibilización y difusión 5. Entrega de información y generación de reportes
<ul style="list-style-type: none"> • Información 	El dato es accesible	Accesibilidad de datos	1. Propiedad de los datos 2. Datos accesibles 3. Caracterización e identificación de oportunidades 4. Medios y canales de acceso 5. Enfoque diferencial 6. Cultura de la información 7. Accesibilidad web 8. Usabilidad web
<ul style="list-style-type: none"> • Información 	Calidad de los datos	Calidad de los datos y la información	1. Calidad de datos 2. Unidades de información 3. Atributos de calidad 4. Mapa de información 5. Reglas de negocio 6. Medición de la calidad 7. Monitoreo continuo 8. Divulgación y reporte 9. Gestión de hallazgos 10. Calidad en los procesos de desarrollo de software 11. Relación entre proyectos de TI y unidades de información

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 14 de 41

DOMINIO DE ARQUITECTURA	PRINCIPIOS GENERALES DE TI	POLÍTICAS GENERALES	POLÍTICAS ESPECIFICAS
<ul style="list-style-type: none"> Información 	Interoperabilidad y colaboración	Interoperabilidad y colaboración	<ol style="list-style-type: none"> Marco de interoperabilidad Colaboración entre entidades del sector de la inclusión social y la reconciliación Identificación de las necesidades de intercambio de información Determinar el marco legal Acuerdos de intercambio de información Directorio de servicios de intercambio de información Conformidad con las políticas de calidad y seguridad Responsabilidad de las entidades Mantenimiento y mejora Monitoreo y seguimiento Desarrollo de aplicaciones
<ul style="list-style-type: none"> Servicios Tecnológicos 	Servicios compartidos de infraestructura	Servicios compartidos de infraestructura de TI	<ol style="list-style-type: none"> Uso común de la infraestructura de TI Mesa de servicios Catálogo de servicios de TI Acuerdos de nivel de servicio Gestión de las operaciones Medición y mejora del servicio
<ul style="list-style-type: none"> Sistemas de Información Servicios Tecnológicos 	Disponibilidad De La Infraestructura De TI	Disponibilidad de la infraestructura de TI	<ol style="list-style-type: none"> Co - relación entre activos de ti y procesos Gestión de la configuración y activos de TI Gestión de problemas e incidentes Gestión de cambios Almacenamiento y respaldo
<ul style="list-style-type: none"> Uso y Apropiación 	Uso y apropiación de soluciones TI	Uso y apropiación de TI	<ol style="list-style-type: none"> Matriz de interesados Estrategia de uso y apropiación Roles y responsabilidades Uso y apropiación en contratos con componentes de TI Seguimiento


A continuación, se detallan las políticas generales y específicas de TI del Instituto:

5.2.1. Políticas generales de alineación de TI con los objetivos estratégicos

Tabla 2 Listado de políticas de alineación TI con los objetivos estratégicos

Dominio de arquitectura	Principio de TI	Políticas específicas
<ul style="list-style-type: none"> Estrategia TI Gobierno TI 	Alineación de TI con los objetivos estratégicos	<ol style="list-style-type: none"> Plan Estratégico de Tecnología Coherencia con los proyectos de inversión pública nacional Interacción entre TI y las dependencias Gobierno de TI Administración del portafolio de proyectos de TI

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 15 de 41

		6. Alineación entre los sistemas de información y los procesos
--	--	--

Declaración: los planes y proyectos en Tecnologías de la Información y las Comunicaciones deben estar orientados al cumplimiento de los objetivos estratégicos de la entidad y satisfacer las necesidades derivadas de la estrategia misional.

Propósito:

- Lograr flexibilidad y adaptabilidad
- Reconocer las TI como un componente catalizador de ventajas y la importancia que tienen en la contribución al logro de las estrategias de negocio.
- Maximizar la generación de valor.
- Apalancar con eficiencia y celeridad el logro de los objetivos estratégicos mediante el aprovechamiento de las TI.

Ámbito: los planes y proyectos institucionales con componentes TI, están sustentados con base en necesidades reales y buscan apoyar y orientar el cumplimiento de los objetivos estratégicos.

Definición: la alineación se refiere al grado de congruencia e integración entre la misión y la tecnología para crear valor a los beneficiarios, directivos, usuarios, colaboradores, grupos de interés.

Marco de referencia:

- COBIT (Control Objectives for Information and related Technology). Objetivos de Control para Tecnologías de Información y Tecnologías Relacionadas.
- TOGAF (The Open Group Architecture Framework). Marco para Arquitectura Empresarial.
- Modelo Integrado de Planeación y Gestión – MIPG
- G.ES.06 Guía Cómo Estructurar el Plan Estratégico de Tecnologías de la Información – PETI.
- Política de Gobierno Digital. Manual para la implementación de la estrategia de Gobierno Digital.

La tabla siguiente detalla las políticas generales de manejo de información asociadas a las políticas específicas de alineación de TI con los objetivos estratégicos:

¡Antes de imprimir este documento... piense en el medio ambiente!


 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 16 de 41

Tabla 3 Políticas específicas de alineación de TI con los objetivos estratégicos

Política No. 1: Plan Estratégico de Tecnología
<p>El Instituto debe crear un Plan Estratégico de Tecnologías de la Información - PETI, en línea con la estrategia y prioridades misionales, el Plan Nacional de Desarrollo, el Plan Indicativo Sectorial, el Plan Institucional y la política pública de Gobierno Digital. La estrategia debe verse reflejada en el mapa de ruta de proyectos que contemple la transformación desde la situación actual hasta el estado deseado con transiciones incrementales. El plan debe ser comunicado, comprendido y aceptado por toda la entidad y debe ser mejorado y actualizado continuamente.</p>
Política No. 2: Coherencia con los proyectos de inversión pública nacional
<p>Los proyectos de inversión en tecnología que tengan apropiación en el Presupuesto General de la Nación deben ser estructurados, formulados, programados, ejecutados y evaluados siguiendo las directrices establecidas por el Departamento Nacional de Planeación y los entes de política y gestión de información para la administración pública.</p>
Política No. 3: Interacción entre TI y las dependencias
<p>Se deben realizar esfuerzos continuos para lograr involucrar a los directivos en los proyectos de TI, debe haber interacción entre las distintas dependencias, buscar soluciones interfuncionales que favorezcan a toda la entidad y a los beneficiarios que atiende. Los directivos deben conocer las capacidades tecnológicas actuales y el rumbo futuro, las oportunidades que ofrece TI, y qué debe hacer la entidad para capitalizar esas oportunidades.</p>
Política No. 4: Gobierno de TI
<p>La organización de la función de TI se debe hacer teniendo en cuenta el modelo operativo, los requerimientos de personal, segregación de funciones, rendición de cuentas, autoridad, roles, responsabilidades y supervisión. Se debe contar con los mecanismos de gobierno que brinden orientación al equipo directivo respecto de las TI, ejerzan vigilancia sobre TI, determinen las prioridades de inversión, e involucren en los procesos importantes de decisión, distribuyan en cascada los objetivos hacia las dependencias, articulen la estrategia y las operaciones de TI, y se desarrolle confianza y corresponsabilidad entre los procesos y las TI.</p>
Política No. 5: Administración del portafolio de proyectos de TI
<p>Debe existir un control para la gestión de proyectos con componentes de TI, que permita la correcta asignación de prioridades, participación de los interesados, entrega de resultados dentro de los tiempos, presupuesto y calidad acordados, la definición de entregables, aseguramiento de la calidad, aprobación de los usuarios, control de cambios, plan formal de pruebas y el monitoreo de los riesgos y avances. Se debe contar con indicadores que midan el avance de los proyectos y permitan establecer qué tanto el plan de TI está integrado a la estrategia, y posibilita realizar la medición, sobre qué tanto están apoyando los sistemas de información a los procesos. Se debe realizar seguimiento semestral al portafolio de proyectos del PETI para tomar acciones necesarias para que los proyectos avancen de acuerdo con el alcance previsto.</p>
Política No. 6: Alineación entre los sistemas de información y los procesos
<p>Se deben identificar, priorizar, especificar y administrar los requerimientos funcionales y técnicos que cubren el alcance de los sistemas de información. Se deben desarrollar los sistemas apropiados y alineados con el modelo de información y el modelo de aplicaciones, cumplir con la calidad especificada en los requerimientos. Se deben adoptar estándares para el desarrollo y/o adquisición de aplicaciones. Los sistemas de información deben estar en permanente evolución según lo demanda el proceso. Debe existir un plan de mantenimiento de aplicaciones de software. Debe haber una correcta alineación entre los sistemas de información y su soporte a los procesos institucionales, permitiendo medir e identificar el porcentaje de apoyo que TI está brindando a la entidad.</p>

5.2.2. Políticas generales de uso eficiente de los recursos de TI

¡Antes de imprimir este documento... piense en el medio ambiente!


 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 17 de 41

Tabla 4 Listado de políticas de uso eficiente de los recursos de TI

Dominio de arquitectura	Principio de TI	Políticas específicas
<ul style="list-style-type: none"> • Estrategia TI • Gobierno TI 	Uso eficiente de los recursos de TI	<ol style="list-style-type: none"> 1. Estandarización 2. Capacidad de la infraestructura 3. Mantener lo simple y funcional 4. Tecnología verde 5. Procesos internos 6. Contratación

Declaración: la Entidad debe establecer mecanismos para el uso eficiente de los recursos de tecnología. Las adquisiciones se deben hacer en razón a necesidades válidas, con base en análisis adecuados y permanentes. Las TI serán dimensionadas para dar soporte a la organización, proporcionando servicios con calidad.

Propósito:

- Realizar inversiones de TI acertadas.
- Mantener altos estándares de calidad y de servicios basados en TI.
- Optimizar la inversión pública en recursos de TI.
- Lograr flexibilidad y adaptabilidad en la prestación de los servicios de TI. □ Minimizar riesgos en la contratación e implantación de TI.

Ámbito: una adecuada infraestructura de TI, altamente adaptada a las necesidades institucionales, permite lograr una mejor integración entre las diferentes dependencias y ayuda a disminuir los costos mediante el uso común de recursos para múltiples áreas funcionales.


La convergencia entre la infraestructura y la prestación de servicios de TI se convierte en un factor crítico de éxito, para garantizar que los servicios se prestan de acuerdo con los requerimientos de los usuarios y permite optimizar y racionalizar el uso de los recursos de TI.

Definición: el uso eficiente de los recursos de TI potencializa la entrega oportuna de servicios basados en TI con los niveles de calidad esperados y una eficiente relación costo– beneficio; permitiendo dar agilidad a los procesos institucionales.

Marco de referencia:

- G.GEN.01 Generalidades del Marco de Referencia de AE para la gestión de TI
- TOGAF (The Open Group Architecture Framework). Marco para Arquitectura Empresarial.
- ITIL (Information Technology Infrastructure Library). Librería de Infraestructura de
- Tecnologías de Información.

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 18 de 41


- Marco de Referencia de Arquitectura TI Colombia. Es el principal instrumento para implementar la Arquitectura TI de Colombia y habilitar la Estrategia de Gobierno Digital.
- Política de Gobierno Digital. Manual para la implementación de la estrategia de Gobierno Digital.

La tabla siguiente detalla las políticas generales de manejo de información asociadas a la Políticas específicas del uso eficiente de los recursos de TI:

Tabla 5 Políticas específicas del uso eficiente de los recursos de TI

Política No. 1: Estandarización
<p>La entidad debe mantener una infraestructura tecnológica uniforme y estandarizada. Se debe encontrar una tendencia a reducir la cantidad de herramientas que satisfacen una misma necesidad para incrementar el nivel de compatibilidad y reducir costos. Toda incorporación de TI debe sumar a la estandarización de la información, las aplicaciones y la infraestructura.</p>
Política No. 2: Capacidad de la infraestructura
<p>La entidad, mediante el proceso de gestión de la capacidad, debe establecer una adecuada capacidad de la infraestructura tecnológica, se debe encargar de monitorear, proyectar y asegurar que la capacidad de la infraestructura de procesamiento y almacenamiento de información, su licenciamiento se debe mantener acorde a las necesidades institucionales y a una oportuna entrega de servicios. Se debe planificar y contratar los recursos con la debida antelación. Los servicios deben estar respaldados por capacidades de procesamiento y almacenamiento suficientes y correctamente dimensionados.</p>
Política No. 3: Mantener lo simple y funcional
<p>La entidad proyecta en el tiempo la infraestructura base, la cual ha sido acondicionada a su funcionalidad, a sus necesidades y a los servicios de TI; se mantienen y se mejoran los recursos de TI funcionalmente estables y de esta manera se minimizan las probabilidades en entornos de fallas u errores. Se entiende que en ambientes TI de baja complejidad, lo simple y lo funcional perdura.</p>
Política No. 4: Tecnología verde
<p>La entidad debe incentivar la eficiencia en el consumo de energía y de papel utilizando tecnologías respetuosas con el medio ambiente. Mediante métodos de computación en la nube, sistemas de teleconferencia, virtualización, optimización del centro de datos, impresión controlada, reciclaje y correcta disposición de equipos; la entidad demostrará conformidad con los lineamientos ecoeficientes. Se deben utilizar las TI como herramientas que facilitan el teletrabajo, reducen el impacto medioambiental y logran reducción de costos. De forma complementaria, en los procesos contractuales de TI, se deben incluir cláusulas relacionadas con el tema de RAEEs.</p>
Política No. 5: Procesos internos
<p>A través del uso de las TIC, la Entidad debe incorporar a sus procesos internos la racionalización y simplificación de procesos, procedimientos, trámites y servicios digitales. La Entidad debe cumplir los requisitos regulatorios, aprovechando el uso eficiente de las TI y asimilar los marcos políticos – legales y normativos vinculando el uso de tecnologías en sus procesos y planeando a largo plazo su arquitectura de TI.</p>
Política No. 6: Contratación
<p>Las compras y adquisiciones de recursos de tecnologías de la información se deben realizar con base a necesidades reales y a requerimientos específicos, permitiendo unir la inversión de TI a las metas institucionales; se deben definir prioridades institucionales en materia de compras y adquisiciones de TI, estableciendo niveles de gastos presupuestados y coherentes se deben realizar análisis costo – beneficio para la adquisición de nuevas soluciones, los cuales incluyan aspectos de seguridad de la información, riesgo y cumplimiento.</p>

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 19 de 41

Para lograr eficiencia y transparencia en las compras, la entidad debe seguir las políticas de contratación estatal determinadas por la Agencia Nacional de la Contratación Pública-Colombia Compra Eficiente.

5.2.3. Políticas generales de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación, Políticas generales de manejo de información.

Tabla 6 Listado de políticas de seguridad de la información


Dominio de arquitectura	Principio de TI	Políticas específicas
<ul style="list-style-type: none"> Gobierno TI Información Sistemas de Información Servicios Tecnológicos 	Seguridad de la información	<ol style="list-style-type: none"> Seguridad de los Recursos Humanos Gestión de Activos Control de Acceso Criptografía Seguridad Física y del Entorno Seguridad de las Operaciones Seguridad de las Comunicaciones Seguridad para la Adquisición, Desarrollo y Mantenimiento de Sistemas Seguridad para Relación con los Proveedores Gestión de Incidentes de Seguridad de la Información
<ul style="list-style-type: none"> Sistemas de Información Servicios Tecnológicos 	Seguridad de la información	<ol style="list-style-type: none"> Continuidad de la Operación Cumplimiento

Declaración: el ICBF protege, preserva y administra la integridad, confidencialidad, disponibilidad y autenticidad de la información, así como la seguridad digital y la gestión de la continuidad de la operación, conforme al mapa de procesos y en cumplimiento de los requisitos legales y reglamentarios, previniendo incidentes mediante la gestión de riesgos integrales en seguridad y privacidad de la información y seguridad digital, con la implementación de controles de seguridad físicos y digitales, orientados a la mejora continua en la gestión y el alto desempeño del Sistema de Gestión de Seguridad de la Información, con la finalidad de prestar servicios con calidad y transparencia a la primera infancia, la niñez, la adolescencia y el bienestar de las familias y comunidades colombianas.

Propósito:

- Brindar mecanismos de aseguramiento para el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información del ICBF.
- Mitigar los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación en el ICBF.

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 20 de 41

- Mitigar los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación en el ICBF.
- Establecer los lineamientos necesarios para el manejo de la información y los recursos tecnológicos del ICBF.

Ámbito: la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación y las Políticas Generales de Manejo aplica donde el Instituto Colombiano de Bienestar Familiar - ICBF tenga presencia o desarrolle 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.

Definición: todos los aspectos relacionados con la definición, el logro y el mantenimiento de la confidencialidad, integridad, disponibilidad y autenticidad de la información.

Marco de referencia:

Modelo de Seguridad y Privacidad de la Información.

- **NTC-ISO/IEC 27000:2017:** Tecnología de la información, técnicas de seguridad, Sistemas de gestión de la seguridad de la información. Visión general y vocabulario
- **NTC-ISO/IEC 27001:2013:** Tecnología de la Información, técnicas de seguridad, sistemas de gestión de seguridad de la Información (SGSI) Requisitos
- **GTC-ISO/IEC 27002:2013:** Tecnología de la información. Técnicas de seguridad. Código de buenas prácticas para la gestión de la seguridad de la información **NTC-ISO/IEC 27005:2011:** Gestión del Riesgo en la Seguridad de la Información
- **NTC-ISO/IEC 27035:2012:** Tecnología de la Información. Técnicas de Seguridad. Gestión de Incidentes de Seguridad de la Información **ISO 22301:2019** Gestión de Continuidad del Negocio.
- **ISO 31000:2018:** Gestión de Riesgos.

La tabla siguiente detalla las políticas generales de manejo de información asociadas a la política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación:


Tabla 7 Políticas específicas de seguridad de la información

Política No. 1: Seguridad de los recursos humanos

El ICBF a través de la Dirección de Gestión Humana debe propender que los servidores públicos entiendan sus responsabilidades frente a la seguridad de la información con el fin de reducir el riesgo de robo, fraude, mal uso de las instalaciones y medios, asegurando la confidencialidad, disponibilidad e integridad de la información.

La Dirección de Contratación deberá incluir en las minutas de los contratistas cualquiera que sea su modalidad, las cláusulas u obligaciones correspondientes al Eje de Seguridad de la Información con el

¡Antes de imprimir este documento... piense en el medio ambiente!

	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 21 de 41

fin de reducir el riesgo de robo, fraude, mal uso de las instalaciones y medios, asegurando la confidencialidad, disponibilidad e integridad de la información.

Política No. 2: Gestión de activos

El Instituto Colombiano de Bienestar Familiar a través de la Dirección de Información y Tecnología, establecerá y divulgará los lineamientos específicos para la identificación, clasificación y buen uso de los activos de información, con el objetivo de garantizar su protección.

Los activos del ICBF deben ser identificados, clasificados y controlados para garantizar su uso adecuado, protección y la recuperación ante desastres. Por tal motivo, se debe llevar el inventario de los activos de información de propiedad del ICBF, discriminado por procesos, regionales y Centros Zonales, de acuerdo con la **G10.GTI - Guía para el Desarrollo de Inventario y Clasificación de Activos**

Con el objetivo de establecer los controles de seguridad físicos y digitales, las dependencias que tienen la custodia de la información generada en el marco de su función, se encargarán proteger la información, de mantener y actualizar el inventario de activos de información relacionados con sus servicios (Información, software, hardware y recurso humano).

La clasificación de la información del ICBF está definida de conformidad con la Ley 1712 de 2014 reglamentada por el Capítulo 2 del Título 1 de la Parte 1 del Decreto 1081 de 2015, la Ley 594 de 2000 (Ley General de Archivos), el Decreto 1080 de 2015 y lo estipulado en la Guía para el Desarrollo de Inventario y Clasificación de Activos del ICBF, regulada por la Guía para la Rotulación de la Información.

Todos los colaboradores que hagan uso de los activos de información del ICBF tienen la responsabilidad de cumplir las políticas establecidas para su uso aceptable, entendiendo que el uso no adecuado de los recursos pone en riesgo la continuidad de la operación y por ende el cumplimiento de la misión institucional.

Política No. 3: Control de acceso

Los propietarios de los activos de información deben establecer medidas de control de acceso a nivel de red, sistema operativo, sistemas de información, servicios de tecnologías de la información e infraestructura física con el fin de mitigar riesgos asociados al acceso a la información y servicios de infraestructura tecnológica de personal no autorizado, salvaguardando la integridad, disponibilidad y confidencialidad de la información del ICBF.

Política no. 4: Criptografía

La Dirección de Información y Tecnología deberá contar con controles en el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, integridad y disponibilidad de la información.


Política No. 5: Seguridad física y del entorno

El ICBF debe contar con controles para la protección del perímetro de seguridad de las instalaciones físicas, controlar el acceso del personal y la permanencia en las oficinas e instalaciones, así como controlar el acceso a áreas restringidas (áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones), además mitigar los riesgos y amenazas externas y ambientales, con el fin de evitar afectación la confidencialidad, disponibilidad e integridad de la información de la Entidad.

Todos los funcionarios, contratistas y visitantes que se encuentren en las instalaciones físicas del ICBF deben estar debidamente identificados, con un documento que acredite su tipo de vinculación, el cual deberá portarse en un lugar visible.

Los visitantes en el ICBF siempre deben permanecer acompañados por un funcionario o contratista debidamente identificado.

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 22 de 41

El personal de empresas contratistas que desempeñen funciones de forma permanente en las instalaciones del ICBF, debe estar identificado con carné y chalecos o distintivos del Contratista y portar el carné de la ARL.

Política No. 6: Seguridad de las operaciones

La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos será la encargada de la operación y administración de los recursos tecnológicos que soportan la operación del ICBF, así mismo, velará por la eficiencia de los controles asociados a los recursos tecnológicos protegiendo la confidencialidad, integridad y disponibilidad de la información, así como, la de asegurar que los cambios efectuados sobre los recursos tecnológicos, serán controlados y debidamente autorizados. De igual manera, deberá proveer la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información del ICBF, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica de acuerdo con el crecimiento de la Entidad.

La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos deberá realizar y mantener copias de seguridad de la información de la Entidad en medio digital, siempre que ésta sea reportada por el responsable de esta, con el objetivo de recuperarla en caso de cualquier tipo de falla, ya sea de hardware, software, o de procedimientos operativos al interior de la Entidad.

Se efectuará la copia respectiva de acuerdo con el esquema definido previamente en el documento Procedimiento Gestión Copias de Seguridad de la Entidad, el cual deberá ser diseñado por la Subdirección de Recursos Tecnológicos, en conjunto con los líderes de Proceso.

Política No. 7: Seguridad de las comunicaciones


La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos, establecerá los mecanismos necesarios para proveer la disponibilidad de las redes y de los servicios que dependen de ellas; así mismo, dispondrá y monitoreará los mecanismos necesarios de seguridad para proteger la integridad y la confidencialidad de la información del ICBF.

Como parte de sus términos y condiciones iniciales de trabajo, los funcionarios o contratistas, cualquiera sea su nivel jerárquico dentro de la entidad, firmarán un Compromiso de Confidencialidad y no divulgación, en lo que respecta al tratamiento de la información de la Entidad, y de igual manera la Autorización de tratamiento de datos personales, en los términos de la Ley 1581 de 2012, así como el capítulo 25 del Decreto 1074 de 2015 y la Ley 1712 de 2014 reglamentada por el capítulo 2 del Decreto 1081 de 2015 y las demás normas que las adicionen, modifiquen, reglamenten o complementen. Dicho compromiso y Autorización (documento original) deberá ser retenido en forma segura por la Dirección de Gestión Humana (funcionarios), la Dirección de Contratación (contratistas) o quien haga las veces en las Direcciones Regionales, según el caso. Así mismo, mediante el Compromiso de Confidencialidad el funcionario o el contratista declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad ni los derechos del funcionario o contratista.

En el caso de que sea personal que ejecute tareas propias del ICBF y haya sido contratado en el marco de un contrato o convenio con el ICBF, debe reposar en la carpeta de ejecución del contrato un compromiso de confidencialidad debidamente suscrito por el Representante Legal de la empresa contratista o con la cual se realiza el convenio.

Política No. 8: Seguridad para la adquisición, desarrollo y mantenimiento de sistemas

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 23 de 41

La Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de información velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad adecuados para la protección de la información del ICBF.

La Dirección de Información y Tecnología será la única dependencia de la Entidad con la capacidad de adquirir, desarrollar o avalar la adquisición y recepción de software de cualquier tipo, conforme a los requerimientos de las diferentes dependencias, con el fin de garantizar la conveniencia, soporte, mantenimiento y seguridad de la información de los sistemas que operan en el Instituto.

En consecuencia, cualquier software que opere en el Instituto y no haya sido entregado a la Dirección de Información y Tecnología, no serán responsabilidad de esta, no se le brindará soporte y no se le salvaguardará la información.

Política No. 9: Seguridad para relación con proveedores

El ICBF establecerá mecanismos de control en relaciones con sus proveedores, teniendo en cuenta que se debe asegurar la información a la que tengan acceso, supervisando el cumplimiento de lo establecido en el Eje de seguridad de la información. Los Supervisores de los contratos o convenios en conjunto con la Dirección de Información y Tecnología, tendrán la responsabilidad de la divulgación de las políticas y procedimientos de la seguridad de la información.

Política No. 10: Gestión de incidentes de seguridad de la información

El ICBF promoverá entre los funcionarios y contratistas el reporte de incidentes relacionados con la seguridad de la información y sus medios, reporte y seguimiento. Así mismo, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, de acuerdo con su criticidad. El Director General o a quien éste delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas, medios de comunicación o la ciudadanía.

Política No. 11: Continuidad de la operación

El ICBF dispondrá los planes necesarios para la implementación del proceso de continuidad de la operación, el cual será operado por los líderes de los procesos del modelo de operación, la cual deberá contar lo establecido en el Análisis de Impacto a la Operación (BIA); además, la infraestructura tecnológica necesaria para soportarlos, con el fin de ofrecer continuidad de la operación misional en el marco del cumplimiento del mandato legal.

Política No. 12: Cumplimiento

El ICBF velará por la identificación, documentación y cumplimiento de los requisitos legales enmarcados en la seguridad de la información del Estado Colombiano, entre ella la referente a derechos de autor y propiedad intelectual, protección de datos personales, ley de transparencia y del derecho de acceso a la información pública nacional y las consignadas en la Matriz de Requisitos Legales del ICBF.


El plan de continuidad de tecnologías deberá incluirse en el Plan de Continuidad de la Operación del ICBF, Planes de Emergencia y Contingencia, así como cualquier estrategia alineada a la continuidad de la prestación del servicio de Bienestar Familiar.

5.2.4. Políticas generales de gobierno de datos e información

Tabla 8 Listado de políticas de gobierno de datos e información

Dominio de arquitectura	Principio de TI	Políticas específicas
<ul style="list-style-type: none"> ● Información 	El dato es un activo y se gobierna	<ol style="list-style-type: none"> 1. Gobierno de los datos 2. Responsabilidad compartida 3. Toma de consciencia 4. Organización del gobierno de datos 5. Identificación y caracterización de datos 6. Auditoria, medición y mejora

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 24 de 41

		7. Decisiones basadas en Información
--	--	--------------------------------------

Declaración: los datos de la entidad son activos intangibles de muy alto valor y como tal se les debe proveer el tratamiento correspondiente a la recolección, uso, gestión y suministro preciso y oportuno de los mismos.


Propósito:

- Crear estructuras para la toma de decisiones sobre los activos de información
- Crear y mantener el ciclo de vida de los datos y de la información.
- Responder eficientemente a las necesidades de las áreas que gestionan y utilizan los datos y la información de la entidad
- Adoptar enfoques comunes en lo que respecta a los problemas de los datos.
- Adoptar estándares y desarrollar procesos repetibles para el manejo de los datos y de la información en la entidad.
- Reducir costos y aumentar la eficacia institucional mediante la coordinación de esfuerzos para la administración, gestión y control de la información.
- Garantizar la transparencia de los procesos.
- Permitir la trazabilidad de la información.
- Garantizar la calidad, seguridad y privacidad de los datos de la entidad

Ámbito: el gobierno de datos e información aplica para toda aquella información denominada como estructurada y que se puede encontrar en los datos maestros, metadatos, datos analíticos, datos operacionales de la entidad; adicionalmente, aplica para toda aquella información no estructurada y que se encuentra debidamente identificada y clasificada según su criticidad.

Definición: el gobierno de los datos y de la información, es un sistema de derechos de decisión y rendición de cuentas para que los procesos relacionados puedan utilizar la información de forma tal que éstos se ejecuten según lo definido en los modelos que describen los criterios y los responsables para realizar las acciones correspondientes según las circunstancias presentadas, siguiendo métodos documentados. De tal manera que la gestión de la información se ejecute según lo acordado en los modelos que describen: quién puede tomar las acciones, con cuál información, cuándo, en qué circunstancias y con cuáles métodos. Conforme al artículo 2.2.2.25.4.4 del Decreto 1074 de 2015, que establece la necesidad de contar con un área o persona que asuma como Oficial de Protección de Datos Personales en el ICBF, esta función está liderada por la Dirección de Planeación y Control de Gestión, que tiene como función velar por la implementación efectiva de las políticas y

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 25 de 41

procedimientos adoptados por el Instituto para cumplir las normas, como se contempla en la Circular No. 013 del 14 de diciembre de 2017 suscrita por este Instituto.

Marcos de referencia:


- COBIT (Control Objectives for Information and related Technology). Objetivos de Control para Tecnologías de Información y Tecnologías Relacionadas.
- ITIL (Information Technology Infrastructure Library). Librería de Infraestructura de Tecnologías de Información.
- TOGAF (The Open Group Architecture Framework). Marco para Arquitectura Empresarial.

La tabla siguiente detalla las políticas generales de manejo de información asociadas a las Políticas específicas de gobierno de datos e información:

Tabla 9 Políticas específicas de gobierno de datos e información

Política No. 1: Gobierno de los datos
<p>La entidad debe contar con prácticas para el gobierno de los datos, lo que garantiza que los datos se creen, gestionen y protejan como un recurso valioso para la entidad. El programa de gobierno de datos debe comprometer la articulación de personas, procesos y tecnologías dentro de la entidad para darle así a los datos y a la información el valor que realmente deben tener. Su objetivo es instrumentar un efectivo control de la información.</p> <p>Es responsabilidad del gobierno de datos cumplir con los principios de calidad, seguridad, privacidad y accesibilidad de la información.</p>
Política No. 2: Responsabilidad compartida
<p>El gobierno de la información en la entidad debe garantizar que las decisiones que toman los líderes de procesos se soporten en la implementación eficiente de las guías de los responsables de TI y de información; y que las decisiones técnicas que toman los responsables de TI se soporten en los aportes y en la implementación eficiente de las guías por parte de los usuarios de diferentes niveles. Los propietarios de los datos deben ser los líderes de los procesos, quienes representan los intereses de la entidad respecto de los datos y asumen la responsabilidad respecto de la calidad, seguridad, privacidad, autenticidad y uso de estos, a su vez, deben definir las reglas de negocio para cumplir con las expectativas de las diferentes dependencias de la entidad y de los clientes externos.</p> <p>En la Dirección de Información y Tecnología se deben proporcionar las estructuras, tecnologías y herramientas de bases de datos, y son quienes traducen las necesidades de los dueños de los datos en requisitos tecnológicos. Así mismo, la entidad debe tener definidas las responsabilidades de todos los actores que intervienen en la gestión de los datos y de la información institucional.</p>
Política No. 3: Toma de conciencia
<p>Todos los colaboradores de la entidad deben conocer acerca del gobierno de información y datos y son conscientes de la importancia de la administración de estos.</p> <p>Así mismo, todos los colaboradores deben valorar el rol estratégico de la información; y ser conscientes de los datos y la información a su cargo, así como los procesos de la entidad que los crean, almacenan, procesan y utilizan son de propiedad de la entidad.</p>
Política No. 4: Organización del gobierno de los datos

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 26 de 41

La entidad debe contar con una unidad rectora de coordinación y mecanismo de gobierno que trabaja articuladamente con los dueños de los procesos y los responsables de TI, para definir planes de acción y actividades que tengan como objetivo la mejora continua de la información. Debe haber una estructura con roles definidos que describe los responsables del programa, quiénes y cómo se gestionan las prioridades y se hace seguimiento a su implementación para asegurar que los datos cumplan con las expectativas de las partes interesadas.

Esta unidad rectora debe establecer y aplicar los mecanismos para la gestión y manejo de excepciones o situaciones que incumplan la política.

Política No. 5: Identificación y caracterización de datos

La entidad debe tener definidos los datos que van a ser gobernados, estos a su vez deben ser actualizados permanentemente en el inventario, este inventario permite facilitar a todos los interesados catálogos electrónicos en los que se pueda consultar o acceder fácilmente a la información allí relacionada, también deben existir diccionarios de datos para estandarizar la terminología y manejar un vocabulario común.

La entidad debe tener definidos los propietarios de los datos, los responsables de tomar acciones sobre ellos, el momento, las circunstancias y los métodos con los que debe actuarse.

Política No. 6: Auditoría, medición y mejora

La entidad debe tener establecidas las metas y los indicadores para medir la efectividad del programa de gobierno de información y de datos y de los procesos asociados. Así mismo, periódicamente debe implementar acciones de auditoría de información. Tanto las metas, como los resultados de las auditorías, como de las mediciones deben ser comunicados.

Política No. 7: Decisiones basadas en información

Todas las decisiones de política pública, de funcionamiento interno y de servicio interno y externo se deben soportar en información de calidad, debidamente gestionada, auditada, controlada y publicada; para asegurar así la toma de decisiones de manera objetiva y coherente.

5.2.5. Políticas generales el dato público es compartido

Tabla 10 Listado políticas de dato público compartido


Dominio de arquitectura	Principio de TI	Políticas específicas
<ul style="list-style-type: none"> ● Información 	El dato es público compartido	<ol style="list-style-type: none"> 1. Concordancia con las Políticas de Seguridad de la Información 2. Apertura de datos 3. Divulgación activa de la información pública 4. Sensibilización y difusión 5. Entrega de información y generación de reportes

Declaración: los datos de la entidad que estén clasificados como públicos, deben ser compartidos para lograr mayor eficiencia en los procesos como muestra de transparencia y forma de buen gobierno. Los datos públicos pueden ser publicados sin restricciones de privacidad.

Propósito:

- Mejorar la toma de decisiones
- Cumplir la normatividad vigente
- Obtener transparencia y buen gobierno
- Lograr eficiencia administrativa

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 27 de 41

- Estandarizar los datos de la entidad
- Reutilizar de la información

Ámbito: todos aquellos datos catalogados como públicos, y que, por ende, no estén sometidos a reserva de acuerdo con la constitución y la ley; son susceptibles de ser compartidos y de conocimiento general para la población.

Definición: el dato público hace referencia a información de libre conocimiento y uso, la cual por su designación de “publica” puede circular sin ningún tipo de restricción.

Marcos de referencia:

- **Decreto No. 1008 de 2018:** *"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"*. Constitución política de Colombia. 1991.
- World Wide Web Consortium (W3C)
- Metodología para la implementación del modelo integrado de planeación y de gestión.


La tabla siguiente detalla las políticas generales de manejo de información asociadas a las Políticas específicas de dato público compartido:

Tabla 11 Políticas específicas de dato público compartido

Política No. 1: Concordancia con las políticas de seguridad de la información
<p>En concordancia con la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, la entidad debe contar con el inventario de clasificación de la información y tener identificada con claridad la información catalogada como “pública”.</p>
Política No. 2: Apertura de datos
<p>La entidad, previo análisis interno del proceso de calidad y legalidad, debe abrir sus datos primarios, sin procesar, en formatos estándar, estructurados e interoperables; de tal manera que se facilita su acceso, control, reutilización, sin ninguna reserva de forma libre y sin restricciones, con el fin que terceros puedan reutilizarlos y crear servicios y aplicaciones que agreguen valor a la ciudadanía y a la sociedad en general, así como, que permitan el control y fomenten la transparencia, la eficiencia y la eficacia institucional.</p>
Política No. 3: Divulgación activa de la información pública
<p>La entidad debe cumplir con la obligación correlativa de realizar una activa divulgación de la información catalogada como pública (según los medios y canales de acceso definidos y dispuestos), en cumplimiento del derecho de acceso a la información y en concordancia con el componente de transparencia, participación y servicio al ciudadano; del modelo integrado de planeación y de gestión.</p>
Política No. 4: Sensibilización y difusión
<p>Los funcionarios de la entidad deben ser conscientes de la importancia de los datos públicos y asimilar la premisa sobre la cual: “toda la información producida por el estado es pública, salvo aquella con restricciones constitucionales o legales” ¹⁷.</p>

¹⁷ Tomado de: Metodología para la implementación del modelo integrado de planeación y de gestión.

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 28 de 41

Política No. 5: Entrega de información y generación de reportes

La entrega de información pública se debe realizar en el marco de la reglamentación legal vigente, siendo solicitada por peticionarios, mediante rendición de cuentas u obrando bajo la observancia de la transparencia activa en la función pública, por ello la entidad debe definir los responsables, medios y formas de entrega y reporte.

5.2.6. Políticas generales de accesibilidad de datos

Tabla 12 Listado de políticas de accesibilidad de datos

Dominio de arquitectura	Principio de TI	Políticas específicas
<ul style="list-style-type: none"> • Información 	El dato es accesible	<ol style="list-style-type: none"> 1. Propiedad de los datos 2. Datos accesibles 3. Caracterización e identificación de oportunidades 4. Medios y canales de acceso 5. Enfoque diferencial 6. Cultura de la información 7. Accesibilidad web 8. Usabilidad web

Declaración: los datos de la entidad se deben encontrar a disposición de quienes deben acceder a ellos, ya sea para los usuarios, procesos o aplicaciones, en calidad de información pública accesible y transparente para toda la ciudadanía y con enfoque diferencial, presentada en los sitios web institucionales con la aplicación de estándares de accesibilidad y usabilidad.

Propósito:


- Lograr oportunidad en la toma de decisiones
- Generar transparencia y buen gobierno
- Cumplir con la normatividad legal vigente
- Conseguir inclusión con enfoque diferencial
- Focalizar la oferta del ICBF

Ámbito: acceso a los datos institucionales, en calidad de información pública para la ciudadanía, con adecuados niveles de seguridad de la información y en coherencia con su clasificación, así como con la aplicación de estándares mínimos requeridos para accesibilidad y usabilidad a través de sitios web institucionales.

Definición: la accesibilidad y usabilidad permiten el acceso y la facilidad de uso de los datos, información, sistemas de información y portales web independientemente de las capacidades de los usuarios, el tipo de tecnología y las características demográficas, geográficas, intrínsecas y de comportamiento.

Marcos de referencia:

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 29 de 41


- ISO 27001:2013
- NTC 5854 World Wide Web Consortium (W3C) Niveles mínimos A y AA referidos en el Anexo 1 de la Resolución No. 1519 de 2020.
- Lineamientos y políticas establecidas por el Min TIC
- World Wide Web Consortium (W3C)
- Política de Gobierno Digital (Decreto 1008 de 2018)
- Ley de Transparencia y Acceso a Información Pública (Ley 1712 de 2014)

La tabla siguiente detalla las políticas generales de manejo de información asociadas a las Políticas específicas relacionadas con la accesibilidad de datos:

Tabla 13 Políticas específicas relacionadas con la accesibilidad de datos

Política No. 1: Propiedad de los datos
<p>La entidad debe reconocer su propiedad o la de terceros, sobre los datos producidos, almacenados y/o gestionados; al igual que su responsabilidad sobre la organización, conservación, uso, manejo y publicación de estos. Todo lo anterior, según la reglamentación legal vigente y aplicable.</p>
Política No. 2: Datos accesibles
<p>Se debe contar con las condiciones institucionales que permitan brindar un adecuado nivel de acceso a los datos en cualquiera de sus clasificaciones; los accesos se permiten de forma segura, con niveles de acceso, salvaguardando las responsabilidades y autonomía de la entidad en cuanto a la accesibilidad, mantenimiento y actualización de los datos.</p>
Política No. 3: Caracterización e identificación de oportunidades
<p>La entidad debe entender y conocer las necesidades de sus beneficiarios y partes interesadas en cuanto a la provisión de información y su acceso. Se deben establecer oportunidades de entrega de valor, contribuyendo al incremento de la transparencia en la gestión pública y facilitando el acceso a la información pública.</p>
Política No. 4: Medios y canales de acceso
<p>Se deben tener identificados e implementados los medios y canales apropiados para brindar mecanismos de acceso a los datos; las consultas y accesos a datos públicos que son gratuitos. Se debe realizar monitoreo, identificar oportunidades de mejora y optimizar los mecanismos de acceso para los actores que puedan consultar los datos. Se debe disponer de sistemas de información efectivos que permiten al ciudadano un fácil acceso a la información.</p>
Política No. 5: Enfoque diferencial
<p>El acceso a los datos se debe brindar mediante la caracterización de usuarios del tipo de servicio o trámite. Se debe acoger la clasificación determinada por el Modelo de Enfoque Diferencial de derechos que contempla cuatro categorías: (i) Étnica, (ii) Discapacidad, (iii) Género y (iv) Diversidad Sexual, adoptado por ICBF por Resolución 1264 de 2017, respecto de la atención preferencial que por mandato de ley deben tener algunos sujetos especiales identificados dentro de nuestra sociedad y a los requisitos preferenciales y diferenciales de acceso, según el grupo al que pertenece el sujeto protegido. El ICBF debe entender el enfoque diferencial como un aporte del derecho internacional de los derechos humanos a la implementación de políticas públicas, buscando que el centro de la intervención social esté dado por las características del sujeto social y su contexto. El acceso brindado mediante medios y canales electrónicos y/o tecnológicos, debe tener en cuenta rutas de acceso acordes con los sujetos existentes y para los cuales la entidad brinda oferta institucional.</p>

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 30 de 41

Política No. 6: Cultura de la información

En la entidad, la información pública se debe valorar como un bien y todos los servidores públicos deben asumir que es propiedad del Estado y de la ciudadanía. Debe existir la cultura de la correcta y crítica generación, gestión, valoración, análisis y evaluación de la información, de tal manera que permita otorgarle utilidad y uso según su contexto, y al ser la información pública generada a partir del desarrollo de actividades propias del funcionamiento institucional es socializada, difundida y utilizada para la toma de decisiones, la eficacia institucional y la rendición de cuentas por medios electrónicos.

Política No. 7: Accesibilidad web (*)

El ICBF en desarrollo de su misión y en consecuencia del derecho de acceso a la información pública que le aplica como entidad del estado colombiano, garantiza que sus grupos de valor e interés independientemente de sus características o capacidades puedan acceder, navegar y consultar a través del sitio web institucional la información pública de su competencia, todo enmarcado en el cumplimiento de las políticas establecidas por el Sistema de Gestión de Seguridad de Información implementado en la entidad. De igual forma, permite que los usuarios puedan acceder a los canales digitales para orientación y atención, considerando que el acceso a la información pública es un derecho constitucional.

Política No. 8: Usabilidad web (*)

En ejercicio de los deberes contenidos como sujeto obligado en la Ley 1712 de 2014 y la Política de Gobierno Digital, el ICBF implementa estrategias para la evolución y mejora en la aplicación de estándares de usabilidad en los sitios web institucionales del ICBF, que garanticen el cumplimiento de las directrices vigentes en cuanto a la disposición y publicación de información pública de la entidad para la ciudadanía, permitiendo que su sitio web sea correctamente percibido, entendido, navegable e interactivo.

(*) Las políticas de Accesibilidad y Usabilidad Web se alinean y dan cumplimiento a las políticas establecidas por el Sistema de Gestión de Seguridad de Información implementado en la entidad.


5.2.7. Políticas generales de calidad de los datos y la información

Tabla 14 Listado de políticas de calidad de los datos y la información

Dominio de arquitectura	Principio de TI	Políticas específicas
<ul style="list-style-type: none"> • Información 	Calidad de los datos	<ol style="list-style-type: none"> 1. Calidad de datos 2. Unidades de información 3. Atributos de calidad 4. Mapa de información 5. Reglas de negocio 6. Medición de la calidad 7. Monitoreo continuo 8. Divulgación y reporte 9. Gestión de hallazgos 10. Calidad en los procesos de desarrollo de software 11. Relación entre proyectos de TI y unidades de información

Declaración: Los datos deben ser completos, correctos, reflejar la realidad de lo que está pasando en la entidad, ser aptos para su uso y cumplir con un conjunto de atributos.

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 31 de 41

Propósito:

- Maximizar el valor de la información
- Generar confianza en la información institucional
- Cualificar los datos y la información institucional y sectorial Contar con mejores recursos para la toma de decisiones.
- Cumplir los lineamientos y normativas referentes
- Fomentar la transparencia, la probidad, el buen gobierno y la eficiencia administrativa

Ámbito: la información contenida en las bases de datos, en los sistemas de información, de tipo estructurada, debe contar con las condiciones de calidad y oportunidad que permitan a la entidad tomar decisiones y tener una panorámica real de la situación en la cual se encuentra y de los servicios que ofrece.

Definición: la calidad de la información es una propiedad orientada a asegurar que la situación actual de la entidad es válidamente reflejada en la información producida y gestionada, permitiendo altos niveles de aceptación y de confianza en los dueños de la información, en los usuarios y demás partes interesadas.

Marcos de referencia:

- G.INF.01 Básica de Información
- G.INF.02 Guía Técnica de Información - Administración del dato maestro. MinTIC.
- G.INF.03 Ciclo de vida del dato.
- G.INF.04 Migración de datos.
- G.INF.05 Gobierno del dato.
- G.INF.06 Catálogo de componentes de información.
- Guía de estándares de calidad e interoperabilidad de los datos abiertos del gobierno de Colombia. MinTIC.
- MDM (Master Data Management) Gestión de Datos Maestros.
- DMBOX (Data Management Book of Knowledge). Marco de referencia para la Gobernabilidad de Datos.

La tabla siguiente detalla las políticas generales de manejo de información asociadas a las Políticas específicas de calidad de los datos y la información:


Tabla 15 Políticas específicas de calidad de los datos y la información

Política No. 1: Calidad de datos

Se debe contar con prácticas para evaluar y mejorar la calidad de la información producida por las diferentes áreas y que es utilizada con el fin de contar con información real y apta para su uso y de esta forma mantener la calidad de los datos a través del tiempo. Las actividades se deben realizar de forma continua, metódica, iterativa e incremental.

Política No. 2: Unidades de información

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 32 de 41

La entidad debe contar con un inventario actualizado de las unidades de información relevantes y recurrentemente usadas por los procesos seleccionados y priorizados según el mapa de procesos. Las unidades de información se deben encontrar clasificadas de acuerdo con los niveles de acceso y sus dueños estar claramente identificados.

Política No. 3: Atributos de calidad

La entidad debe definir y establecer los atributos de calidad de la información, estos deben estar asociados a cada una de las unidades de información que son identificadas y posteriormente valoradas según el cumplimiento de cada uno de los atributos.

Política No. 4: Mapa de información

La entidad debe contar con el mapa de información, que incluye las unidades de información y su evaluación según los atributos, el mapa de información debe indicar la relación directa entre los procesos y las unidades de información identificadas y valoradas en cada proceso.

Política No. 5: Reglas de negocio

La entidad debe tener definidos e implementados los criterios de validación para verificar que una unidad de información cumple o no con los criterios especificados para un determinado atributo de calidad. También se deben describir las reglas para corregir una unidad de información de acuerdo con los criterios mínimos especificados para un determinado atributo de calidad, cuando se encuentran deficiencias. La corrección de unidades puede incluir tareas automáticas, semiautomáticas, manuales y pueden estar referidas a procesos, personas o tecnologías. Tanto las reglas de validación como las reglas de corrección son acordadas con los dueños de procesos de la entidad y se monitorean constantemente.

Política No. 6: Medición de la calidad

La entidad debe obtener la valoración cualitativa y cuantitativa del estado actual de la calidad de las unidades de información teniendo en cuenta los atributos definidos. Se debe obtener el índice de calidad de información, por medio de la medición cualitativa en la cual se identifican los estilos de problemas recurrentes, y realizar un análisis de causas para priorizar las acciones correctivas en aquellos atributos y unidades de información relevantes. Por su parte, para calcular la medición cuantitativa del índice de calidad de Información se deben aplicar las reglas de validación de cada uno de los atributos de calidad de la información sobre las unidades de información objeto de la medición. Así mismo, se deben evaluar los datos almacenados en la unidad de información para obtener valores que se salen de lo habitual permitiendo la rápida detección de anomalías y así poder tomar decisiones.

Política No. 7: Monitoreo continuo

La entidad debe inspeccionar continuamente y hacer seguimiento periódico al estado de la calidad de la información, con el fin de constatar las mejoras y emitir los informes requeridos. La entidad debe tener definidas las frecuencias de tiempo para la medición.

Política No. 8: Divulgación y reporte


La entidad debe divulgar de manera periódica el mapa de información y las valoraciones de calidad medidas. Se deben generar reportes sobre la evolución del estado de la calidad de la información en sus valoraciones cualitativa y cuantitativa, basados en el indicador de calidad de información y en las reglas identificadas y que se aplican sobre las unidades de información seleccionadas. Esta divulgación debe ser retroalimentada por los usuarios internos y externos.

Política No. 9: Gestión de hallazgos

La entidad debe contar con procedimientos para tratamiento de hallazgos por lo cual se llevan a cabo las actividades requeridas para solucionar los inconvenientes detectados de calidad, los cuales incluyen personas, procesos y tecnología. Las acciones correctivas deben subsanar las deficiencias encontradas garantizando trazabilidad en la aplicación de los cambios de la información y la posibilidad de dar marcha atrás.

Política No. 10: Calidad en los procesos de desarrollo de software

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 33 de 41

La entidad debe aplicar modelos y estándares para el ciclo de construcción de software, ya sea que el software sea desarrollado internamente o a través de terceros.

Los desarrollos de software para sistemas nuevos o existentes deben ser trazables, estar documentados y desarrollarse en ambiente web. Todos los desarrollos a la medida de propiedad de la entidad deben cumplir con la inscripción ante la Dirección Nacional de Derechos de Autor. Se debe cumplir con las políticas de seguridad e interoperabilidad. Los sistemas de información deben ser sujetos de auditorías de calidad y funcionalidad de manera periódica.

Política No. 11: Relación entre proyectos de TI y unidades de información

Los proyectos de TI que involucren unidades de información definidas deben estar orientados a contribuir con la mejora de dichas unidades de información, traduciendo en requisitos tecnológicos las necesidades de los procesos para mejorar la calidad.

5.2.8. Políticas generales de interoperabilidad y colaboración

Tabla 16 Listado de políticas de interoperabilidad y colaboración

Dominio de arquitectura	Principio de TI	Políticas específicas
<ul style="list-style-type: none"> • Información 	Interoperabilidad colaboración	<ol style="list-style-type: none"> 1. Marco de interoperabilidad 2. Colaboración entre entidades del sector de la inclusión social y la reconciliación 3. Identificación de las necesidades de intercambio de información 4. Determinar el marco legal 5. Acuerdos de intercambio de información 6. Directorio de servicios de intercambio de información 7. Conformidad con las políticas de calidad y seguridad 8. Responsabilidad de las entidades 9. Mantenimiento y mejora 10. Monitoreo y seguimiento 11. Desarrollo de aplicaciones


Declaración: los procesos de la Entidad deben compartir datos y posibilitar el intercambio de información entre ellos, con otras entidades y con el ciudadano.

Propósito: mejorar la eficiencia en los procesos, lograr agilidad y calidad en los servicios, aumentar la transparencia, promover el acceso abierto a la información y proporcionar la información de valor agregado, obtenida cuando se reúnen datos procedentes de diferentes sistemas.

Ámbito: abarca tanto el empleo interno del sistema de información, el intercambio de información entre los procesos y los sistemas de información de la Entidad, con entidades del Sector de la Inclusión Social y la Reconciliación y con otras entidades con las que se establezca convenios o acuerdos, así como el despliegue de servicios externos y en línea a ciudadanos.

Definición: interoperabilidad es la capacidad de las organizaciones para intercambiar información y conocimiento en el marco de sus procesos de negocio para interactuar hacia

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 34 de 41

objetivos mutuamente beneficiosos, con el propósito de facilitar la entrega de servicios en línea a ciudadanos, empresas y a otras entidades, mediante el intercambio de datos entre sus sistemas¹⁸.

En el ICBF, la interoperabilidad también aplica como medio para integrar sus sistemas de información, compartir datos y posibilitar el intercambio de información entre ellos.

Marcos de referencia:

- Marco de interoperabilidad para Gobierno en Línea.
- Política de Gobierno Digital. Manual para la implementación de la estrategia de Gobierno Digital.


La tabla siguiente detalla las políticas generales de manejo de información asociadas a las Políticas específicas relacionadas con la interoperabilidad y colaboración:

Tabla 17 Políticas específicas relacionadas con la interoperabilidad y colaboración

Política No.1: Marco de interoperabilidad
<p>Se deben adoptar los principios, políticas, estándares y recomendaciones establecidos por el Marco de interoperabilidad de MinTIC, el Lenguaje Común de Intercambio de Información y demás documentos y manuales.</p>
Política No. 2: Colaboración entre entidades del sector de la inclusión social y la reconciliación
<p>El ICBF debe compartir la voluntad de colaboración, por parte de los directivos de las entidades dueñas de la información en el sector de la Inclusión Social y la Reconciliación, que facilita los procesos de intercambio de información. La entidad, así como sus dependencias responsables participan en las actividades que se programan para el diseño, desarrollo y operación de los servicios de intercambio de información. Los Directivos avalan los ajustes organizacionales, de procesos, legales y técnicos que se requieran.</p> <p>El equipo humano, los responsables y líderes de interoperabilidad en cada entidad deben tener el compromiso e interés para llevar a cabo las tareas que se determinen para facilitar el intercambio de información, en procura de prestar mejores servicios a los ciudadanos.</p>
Política No. 3: Identificación de las necesidades de intercambio de información
<p>Se deben definir y estar en aplicación los instrumentos para que el Instituto determine cuáles son sus necesidades de intercambio de información de acuerdo con su uso:</p> <ol style="list-style-type: none"> 1. Proveedor: ofrecer información a otra organización. 2. Consumidor: usar información de otra organización. <p>La entidad prioriza los servicios e identifica aquellos que son particularmente demandados o susceptibles de ser demandados por otras entidades.</p> <p>Se deben identificar los procesos de negocio involucrados en proveer o consumir los servicios de intercambio de información, los responsables de esos servicios al interior de la entidad, la información objeto del intercambio, el conjunto de datos que se requiere intercambiar con sus características.</p> <p>Se deben determinar las capacidades requeridas de entrega de información evaluando los canales y las condiciones técnicas disponibles.</p>

¹⁸ Definición tomada del Marco de interoperabilidad para Gobierno Digital

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 35 de 41

Además, se deben definir los ajustes organizacionales y de los procesos involucrados e identificar las necesidades de estandarización dentro de un lenguaje común.

Política No. 4: Determinar el marco legal

Debe existir un marco legal adecuado que le otorga las facultades a la entidad para intercambiar información. En coordinación con la oficina jurídica, se deben dar las directrices y definir los requerimientos legales para el intercambio de información con terceras partes. De acuerdo con el tipo de información que se va a intercambiar, se deben identificar los mecanismos para habilitar el uso o prestación de los servicios y se debe definir la forma en que se prestan o consumen los servicios para que la información de carácter reservado o confidencial sea protegida.

Política No. 5: Acuerdos de intercambio de información

Deben existir acuerdos de participación de carácter oficial entre las entidades involucradas. Estos acuerdos deben establecer las pautas para dicho intercambio, se debe contar con los convenios, cumplimiento de regulación normativa o medios acordados para el intercambio de información y estar definidos según aplique.

Política No. 6: Directorio de servicios de intercambio de información

Se debe contar con un catálogo con los servicios de intercambio de información disponibles con el fin de generar y poner a disposición de las dependencias y entidades que lo soliciten. La entidad pública debe divulgar las fichas de información de los servicios disponibles, en un Directorio de servicios de intercambio de información.

Política No. 7: Conformidad con las políticas de calidad y seguridad

En los servicios de intercambio de información, se debe cumplir con las condiciones de seguridad, calidad y el tratamiento confidencial que aplique. La entidad debe implementar las medidas de seguridad en la transmisión y entrega de la información. Se debe acatar los acuerdos de confidencialidad para salvaguardar la información que así lo requiera y proporcionar las condiciones de almacenamiento de la información intercambiada.

La entidad debe establecer las políticas de seguridad para garantizar la mitigación de los principales riesgos de pérdida de confidencialidad e integridad de la información, así como su uso no autorizado, en los servicios de intercambio de información que consume o presta.

Política No. 8: Responsabilidad de las entidades

La entidad debe tener un responsable de la interoperabilidad, encargada de coordinar y liderar en los temas de intercambio de información.

La entidad debe adaptar y modificar sus procesos e infraestructura tecnológica y realizar los ajustes necesarios a las aplicaciones. Debe brindar las condiciones adecuadas del transporte de información, y las condiciones de tiempo y entrega.

La información por intercambiar debe ser originada por el responsable directo de la información. La entidad debe ser responsable de la información o datos contenidos en sus sistemas o aplicaciones para que la prestación de servicios de intercambio de información cuente y cumpla con el nivel de servicio acordado.

Política No. 9: Mantenimiento y mejora


La entidad debe realizar actividades de evolución, mantenimiento y optimización de la plataforma tecnológica para la prestación y consumo de servicios de intercambio de información.

La entidad tiene en funcionamiento un modelo de mejoramiento continuo, con tendencia a aumentar los servicios de intercambio de información disponibles y a mejorar la calidad de los servicios que presta.

Política No. 10: Monitoreo y seguimiento

La entidad debe evaluar los resultados de la prestación de servicios de intercambio de información y el cumplimiento de los niveles de servicio acordados. A su vez, debe detectar los escenarios de nuevas solicitudes de servicios de intercambio de información de otras entidades, y brindar a las dependencias las herramientas para que conozcan cómo proceder ante tales solicitudes de la forma más eficiente y qué tipo de información puede entregar directamente. Toda la información que manejan las áreas

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 36 de 41

misionales de la entidad debe ser susceptible de ser requerida por otra entidad para mejorar sus servicios.

Política No. 11: Desarrollo de aplicaciones

Siempre que la entidad plantea la adquisición, desarrollo o adaptación de una solución informática, se debe concebir que los datos que administrará la aplicación en cuestión sean intercambiados con otras aplicaciones de la misma entidad o con otras entidades en el futuro. Por principio general, todo sistema de información debe ser susceptible de intercambiar la totalidad o al menos una parte de su información con otros sistemas de información, así esto no sea una necesidad manifiesta en el primer momento en el que se construye la aplicación.

Por esto, ante el desarrollo de cada aplicación, se deben fijar las pautas específicas que dictan qué información será capaz de compartir y cómo lo logrará. Se debe evaluar qué funcionalidades de integración con otras aplicaciones ofrecerá la aplicación, considerando el cumplimiento de los atributos de calidad de los datos y las políticas de calidad. Las aplicaciones deben ser diseñadas de tal manera que garanticen la interoperabilidad, una de las verificaciones se evidencia con la obtención de la certificación de lenguaje común de intercambio de información que permite estandarizar los datos a intercambiar.

5.2.9. Políticas generales de servicios compartidos de infraestructura de TI

Tabla 18 Listado de políticas de servicios compartidos de infraestructura de TI

Dominio de arquitectura	Principio de TI	Políticas específicas
<ul style="list-style-type: none"> • Servicios Tecnológicos 	Servicios compartidos de infraestructura	<ol style="list-style-type: none"> 1. Uso común de la infraestructura de TI 2. Mesa de servicios 3. Catálogo de servicios de TI 4. Acuerdos de nivel de servicio 5. Gestión de las operaciones 6. Medición y mejora del servicio


Declaración: La Entidad debe centralizar las actividades comunes, economizando en recursos humanos, infraestructura, incrementando el mejoramiento de servicio, así mismo contar con una infraestructura tecnológica centralizada, estandarizada y dimensionada para dar soporte a toda la Entidad.

Propósito:

- Mantener altos estándares de calidad y de servicios basados en TI Optimizar la inversión pública en recursos de TI.
- Lograr flexibilidad y adaptabilidad en la infraestructura de TI.
- Mantener una infraestructura TI centralizada y recuperable ante desastres
- Unificar criterios para la inversión en TI.

Ámbito: bajo modelos operativos de infraestructura TI centralizada, las instituciones aprovechan ventajas funcionales que pueden representar mejoras sustanciales en la operación, uso y mantenimiento de la infraestructura; de igual manera se generan sinergias que permiten “el compartir servicios de TI” por todas las áreas y procesos, ello redundando

¡Antes de imprimir este documento... piense en el medio ambiente!

	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 37 de 41

en integraciones de tipo funcional entre los procesos y las TI, reduciendo costos y brindando agilidad.

Definición: los servicios compartidos de infraestructura tecnológica se refieren a la perspectiva de uso común de una misma infraestructura, de unos mismos servicios y de unas mismas capacidades; por diferentes procesos o áreas de una entidad, bajo parámetros institucionales de gobierno y de toma de decisiones.

Marco de referencia


- COBIT (Control Objectives for Information and related Technology). Objetivos de Control para Tecnologías de Información y Tecnologías Relacionadas.
- ITIL (Information Technology Infrastructure Library). Librería de Infraestructura de Tecnologías de Información.
- Marco de Referencia de Arquitectura TI Colombia. Es el principal instrumento para implementar la Arquitectura TI de Colombia y habilitar la Estrategia de Gobierno Digital.
- Política de Gobierno Digital. Manual para la implementación de la estrategia de Gobierno Digital.

La tabla siguiente detalla las políticas asociadas a la política general:

Tabla 19 Políticas específicas de los servicios compartidos de infraestructura de TI

Política No. 1: Uso común de la infraestructura de TI
La infraestructura de TI debe proporcionar servicios para toda la entidad. Se deben brindar servicios confiables a las dependencias, la administración de bases de datos, la infraestructura de redes y los servicios de telecomunicaciones son centralizados y las dependencias hacen uso común de los recursos de TI. La infraestructura de TI debe proporcionar la flexibilidad para el desarrollo de nuevas aplicaciones.
Política No. 2: Mesa de servicios
Debe existir un punto de contacto entre los usuarios y la gestión de TI que atienda las peticiones de los usuarios proporcionándoles información y acceso a los servicios, registre y monitoree los incidentes, aplique soluciones, realice la gestión de requerimientos, sea de fácil acceso para los usuarios y ofrezca servicios homogéneos y de calidad.
Política No. 3: Catálogo de servicios de TI
Se deben encontrar definidos y documentados de forma comprensible para los usuarios, los servicios de TI que la entidad presta actualmente con toda la información de interés referente a la prestación del servicio, objetivo, los acuerdos de nivel de servicio asociados, responsables, proceso al que apoya, horarios, soporte y proveedores externos que involucre.
Política No. 4: Acuerdos de nivel de servicio
Los servicios de TI prestados internamente o por empresas externas se deben ejecutar contra acuerdos de niveles de servicios - ANS equitativos, exigibles y a un costo razonable. La calidad de los servicios debe ser monitorear respecto de los objetivos establecidos en los Acuerdos de Nivel de Servicio.
Política No. 5: Gestión de las operaciones
Permanentemente se deben llevar a cabo las tareas relacionadas con la operación de los componentes de la infraestructura, los servicios prestados y las aplicaciones; de igual manera se deben realizar periódicamente y conforme a requerimientos, los mantenimientos preventivos y ejecutar los correctivos a los que hubiese lugar.

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 38 de 41

Política No. 6: Medición y mejora del servicio

Se deben definir y aplicar los indicadores para medir el progreso, cumplimiento, eficacia y rendimiento de los servicios prestados. La mejora debe ser alcanzada mediante el monitoreo continuo y la medición de actividades y procesos involucrados en la prestación del servicio.

5.2.10. Políticas generales de disponibilidad de la infraestructura de TI

Tabla 20 Listado de políticas de disponibilidad de la infraestructura de TI

Dominio de arquitectura	Principio de TI	Políticas específicas
<ul style="list-style-type: none"> • Sistemas de Información • Servicios Tecnológicos 	Disponibilidad de la infraestructura de TI	<ol style="list-style-type: none"> 1. Co - relación entre activos de ti y procesos 2. Gestión de la configuración y activos de TI 3. Gestión de problemas e incidentes 4. Gestión de cambios 5. Almacenamiento y respaldo

Declaración: la Infraestructura de hardware, software y telecomunicaciones debe estar en funcionamiento y al servicio de los usuarios internos y externos cuando lo requieran.

Propósito:

- Garantizar la normal prestación de servicios de TI
- Mantener altos estándares de calidad y de servicios basados en TI
- Implementar un Plan de recuperación ante desastres con origen en TI
- Implementar esquemas de gobernabilidad TI

Ámbito: la infraestructura de TI se ha convertido en un referente significativo para la adecuada operación organizacional, debido a ello la entidad sustenta y basa importantes procesos en su infraestructura de tecnología de información, a razón de esto ha cobrado la mayor relevancia institucional.


Definición: la disponibilidad de la infraestructura tecnológica hace referencia a la cadena de actividades cíclicas y repetitivas de mantenimiento y actualización; las cuales garantizan que los recursos de TI estén al servicio, en los tiempos o momentos en que son requeridos, por los usuarios internos o externos.

Marco de referencia:

La tabla siguiente detalla las políticas generales de manejo de información asociadas a las políticas específicas de alineación de TI con los objetivos estratégicos:

- ISO/IEC 27001:2013. Sistemas de gestión de seguridad de la Información (SGSI) Requisitos.
- COBIT (Control Objectives for Information and related Technology). Objetivos de Control para Tecnologías de Información y Tecnologías Relacionadas.
- ITIL (Information Technology Infrastructure Library). Librería de Infraestructura de Tecnologías de Información.

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 39 de 41

- NTC/ISO 22301: Sistema de Gestión de Continuidad de Negocio.
- Marco de Referencia de Arquitectura TI Colombia. Es el principal instrumento para implementar la Arquitectura TI de Colombia y habilitar la Estrategia de Gobierno Digital.
- Sistemas de gestión de seguridad de la Información (SGSI) Requisitos.

La tabla siguiente detalla las políticas generales de manejo de información asociadas a las Políticas específicas de disponibilidad de la infraestructura de TI:

Tabla 21 Políticas específicas de disponibilidad de la infraestructura de TI

Política No. 1: Correlación entre activos de TI y procesos
Se debe tener un inventario de los activos de infraestructura de hardware, software y telecomunicaciones por cada uno de los procesos institucionales que habilitan tecnológicamente, teniendo en cuenta el incremento en el apoyo de la entidad en tecnologías de información.
Política No. 2: Gestión de la configuración y activos de TI
Se debe llevar un registro actualizado de todos los elementos que configuran la infraestructura de TI junto con sus interrelaciones: dispositivos de hardware, software y documentación. Cada elemento debe tener asociados sus atributos relevantes. Se debe conocer el estado de cada componente en todo momento durante su ciclo de vida. El registro de los componentes de hardware se debe mantener actualizado y estar correctamente registrado todo el software en producción. Se debe llevar control sobre el estado de las licencias. Se debe mantener actualizada la biblioteca de medios definitivos donde se guardan copias de todo el software en producción.
Política No. 3: Gestión de problemas e incidentes
Se deben resolver de manera rápida y eficaz los incidentes que causen interrupción o reducción de la calidad en el servicio. Cuando los incidentes son recurrentes o tienen un fuerte impacto en la infraestructura de TI, se deben determinar las causas y encontrar posibles soluciones. Se deben manejar niveles de escalamiento, categorización, nivel de prioridad, asignación del personal de soporte técnico y monitorizar el tiempo de respuesta según los acuerdos de nivel de servicio. Se deben detectar las alteraciones en los servicios de TI, registrar y asignar al personal encargado de restaurar el servicio según se considere en los acuerdos de nivel de servicio.
Política No. 4: Gestión de cambios
Cualquier cambio en la infraestructura central de procesamiento de información debe ser planificado y evaluado. Se debe asegurar que este se lleve a cabo de la manera más eficiente siguiendo los procedimientos establecidos y garantizando en todo momento la calidad y continuidad del servicio. Antes de realizar cualquier cambio, este debe ser llevado a un entorno de prueba y puede deshacerse en caso de un incorrecto funcionamiento luego de su implementación.
Política No. 5: Almacenamiento y respaldo
La entidad debe mantener la capacidad para recuperar los datos perdidos luego de un incidente. Deben existir procedimientos para la realización de copias de seguridad que garanticen la recuperación de la información. Según el nivel de criticidad de la información y los volúmenes de información a copiar, se deben aplicar las tecnologías adecuadas, el esquema de respaldo, la frecuencia y el soporte utilizado. Las copias de respaldo deben ser planificadas. Se deben tener definidos y aplicar los mecanismos de comprobación para verificar el estado de la copia. Los medios deben ser guardados en un sitio seguro. Se debe probar periódicamente la confiabilidad del sistema de respaldo.

5.2.11. Políticas generales de uso y apropiación de TI

¡Antes de imprimir este documento... piense en el medio ambiente!


 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 40 de 41

Tabla 22 Listado de políticas de uso y apropiación de TI

Dominio de arquitectura	Principio de TI	Políticas específicas
<ul style="list-style-type: none"> • Uso y Apropiación 	Uso y apropiación de soluciones TI	<ol style="list-style-type: none"> 1. Matriz de interesados 2. Estrategia de uso y apropiación 3. Roles y responsabilidades 4. Uso y apropiación en contratos con componentes de TI 5. Seguimiento

Declaración: el ICBF debe contar con una estrategia de uso y apropiación de TI que aporte al cumplimiento de los objetivos de los proyectos de TI.

Propósito:

- Permitir a los colaboradores y usuarios externos el acceso a aplicaciones y servicios de la Dirección de Información y Tecnología.
- Ofrecer transferencias de conocimiento para el aprovechamiento y uso correcto de servicios de TI.
- Mantener el acceso a la red de la entidad conforme a los principios y políticas de TI, sus procedimientos, guías e instructivos.
- Brindar socialización, sensibilización y apoyo a los colaboradores y usuarios externos, de las nuevas aplicaciones y servicios de la Dirección de Información y Tecnología.
- Generar comportamientos replicables sobre la adopción de la tecnología.
- Alinearse con los demás planes de capacitación, gestión del cambio o cultura de la entidad.
- Incluir los nuevos servicios dentro del catálogo de servicios de TI.

Ámbito: se debe propiciar una estrategia de acercamiento de los colaboradores del ICBF a las herramientas de TI de manera que se generen en ellos capacidades y empatía sobre la oferta de TI en la entidad.

Definición: el uso y apropiación hace referencia a vincular a las personas y desarrollar una cultura o comportamientos culturales que faciliten la adopción de tecnología".

Marco de referencia:


- Marco de Referencia de Arquitectura TI.

La tabla siguiente detalla las políticas generales de manejo de información asociadas a las Políticas específicas de uso y apropiación de TI:

Tabla 23 Políticas específicas de uso y apropiación de TI

Política No. 1: Matriz de interesados

¡Antes de imprimir este documento... piense en el medio ambiente!

 BIENESTAR FAMILIAR	PROCESO DIRECCIONAMIENTO ESTRATÉGICO	A9.MS.DE	18/01/2022
	ANEXO PRINCIPIOS Y POLÍTICAS GENERALES DE TIC	Versión 2	Página 41 de 41

Para lograr definir de manera clara las actividades de uso y Apropiación de TI a realizar, el Instituto debe realizar una identificación de los grupos interesados en la implementación de proyectos de TI.

Política No. 2: Estrategia de uso y apropiación

La entidad debe generar un Plan de Uso y Apropiación de TI que permita fortalecer el uso eficiente de los servicios y herramientas tecnológicas, para generar apropiación de éstas, e incentivar una cultura de TI en los colaboradores del ICBF que facilite una mayor producción e innovación laboral.

Política No. 3: Roles y responsabilidades

El Instituto debe generar roles relacionados con la generación, aprobación, implementación y seguimiento de la Estrategia de Uso y Apropiación, a través de un equipo dedicado a tal fin.

Política No. 4: Uso y apropiación en contratos con componentes de TI

Dentro de los contratos, donaciones o convenios desarrollados por el ICBF, aquellos que tengan componentes de tecnología, deben contener como productos resultados del proceso como mínimo: manuales de usuario, manuales técnicos y transferencia de conocimiento tanto a las áreas funcionales como la DIT/SSII/SRT.

En el caso de nuevas funcionalidades o actualizaciones efectuadas a las aplicaciones, servicios digitales y/o recursos tecnológicos del ICBF, la transferencia de conocimiento debe realizarse al personal técnico que designe la Dirección de Información y Tecnología y al grupo de interés que impacte.

Una vez los grupos de interés reciben la transferencia de conocimiento, estos adquieren el compromiso de replicar en sus áreas el conocimiento adquirido para el aprovechamiento y correcto uso de las aplicaciones, servicios digitales y/o recursos tecnológicos del ICBF.

Política No. 5: Inclusión en el catálogo de TI de la DIT

El Instituto Colombiano de Bienestar Familiar, dentro de su oferta de servicios, provee el catálogo de servicios de la Dirección de información y Tecnología. Luego de entrar en producción un nuevo servicio, aplicativo o herramienta tecnológica, este debe incluirse dentro de dicho catálogo.

Política No. 6: Seguimiento

El ICBF, dentro de sus actividades, debe evaluar el nivel de adopción de tecnología y satisfacción en el uso. Se deben generar indicadores de seguimiento de la implementación del plan de uso y apropiación de TI. Contar con un inventario de herramientas tecnológicas para desarrollar y facilitar la implementación el plan de uso y apropiación de TI.

Promover el uso de un lenguaje claro en las comunicaciones del Instituto hacia los grupos de interés. Las áreas funcionales dueñas de los trámites, servicios digitales o sistemas de información deben caracterizar a los usuarios a quienes atiende para desarrollar interacciones digitales teniendo en cuenta al usuario.

6. CONTROL DE CAMBIOS

Tabla 24 Control de cambios

Fecha	Versión	Descripción del Cambio
03/12/2019	A9.MS.DE Versión 1	<ul style="list-style-type: none"> • Se actualizó el formato de todo el documento. • Se incluyó un contenido de tablas y se modificaron los colores de estas. • Se incluyó la política de accesibilidad y usabilidad alineada al principio general de TI "El dato es accesible". • Se realizó la respectiva descripción, de igual forma, se ajustó la declaración, el ámbito, la definición y los marcos de referencia. • Se incluyó la nota que políticas las políticas de Accesibilidad y Usabilidad Web se alinean y dan cumplimiento a las políticas establecidas por el Sistema de Gestión de Seguridad de Información implementado en la entidad • La política de Usabilidad y Accesibilidad web, fue revisada por el equipo de seguridad de la información.

¡Antes de imprimir este documento... piense en el medio ambiente!