Elaborado por:	Revisado por:	Aprobado por:
Ana Paola Ramírez Luis Fernando Mancera Gerencia Implementación de la Estrategia	Natalia Gutiérrez –Gerente Implementación de la Estrategia	Comité Directivo SIG

TABLA DE CONTENIDO

Nombre del proceso: 17.1 Administración del modelo integral de gestión empresarial

Nombre del procedimiento: 17.1.1 Gestión del modelo operativo

INTRODUCCIÓN

El manual del Sistema Integrado de Gestión (SIG) tiene la responsabilidad de orientar la integración de los sistemas de gestión de ETB mediante la armonización de sus requisitos, objetivos, necesidades entre otros, a fin de optimizar el uso de los recursos y evitar la duplicidad de esfuerzos y funciones. Adicionalmente busca comprometer a la entidad con el mejoramiento continuo para asegurar su permanencia en el negocio.

OBJETIVO

El Manual del Sistema Integrado de Gestión (SIG) es un documento estratégico - dentro de la estructura documental- que tiene por objetivo fundamental describir la estructura del sistema y el mecanismo a través del cual da cumplimiento a los requisitos necesarios para establecer, documentar, implementar y mantener el Sistema Integrado de Gestión.

ALCANCE

El alcance de este manual contempla los ocho sistemas de gestión que actualmente tiene la entidad (Sistema de Gestión de Calidad, Sistema de Gestión de Seguridad de la Información, Sistema de Responsabilidad Social Corporativa, Sistema de Gestión de Riesgos, Sistema de Gestión Ambiental, Sistema de Gestión de Continuidad de Negocio, Sistema de Salud y Seguridad en el Trabajo, Sistema de Gestión Documental).

SISTEMA	ALCANCE	CERTIFICACIÓN
Sistema de Gestión de Calidad	Todos los procesos de la entidad. Nota: Ver alcance en la página 3 de este documento.	Certificado bajo ISO 9001:2008 y NTC GP 1000:2009

Sistema de Gestión de Riesgos	Todos los procesos de la entidad.	No certificado
Sistema de Gestión de Seguridad de la Información	Los procesos ejecutados en los Data Center de Ciudad Universitaria (CUNI) y Santa Bárbara. Nota: Ver alcance en la página 3 de este documento.	Certificado bajo ISO/IEC 27001:2013
Sistema de Gestión de Continuidad de Negocio	Procesos críticos identificados en el BIA	No certificado
Sistema de Gestión Ambiental	Todos los procesos de la entidad en Bogotá Nota: Ver alcance detallado más adelante en documento.	Certificado bajo la norma Iso 14001:2010
Sistema de Gestión de Seguridad y Salud en el trabajo	Todos los procesos de la entidad.	No certificado
Sistema de Gestión de Responsabilidad Corporativa	Todos los procesos de la entidad Nota: Ver alcance más adelante en este documento	Certificado bajo la norma WorldCob CRS:2011.1
Sistema de Gestión Documental	Todos los procesos de la entidad	No certificado

A continuación se describe el alcance de los sistemas que actualmente se encuentran certificados en ETB:

El alcance de la Certificación del Sistema de Gestión de Calidad es:

“Planificación, diseño, comercialización, consultoría, implementación, operación, mantenimiento, facturación, tesorería y gestión en prestación de servicios de telecomunicaciones y de valor agregado para soluciones de transporte electrónico de datos, redes corporativas, canales dedicados, acceso a Internet e integración de soluciones en TIC´s en el ámbito nacional.”

Para el Sistema de Gestión de Seguridad de la Información el alcance de la Certificación es:

“El Sistema de Gestión de Seguridad de la Información (SGSI) de ETB, garantiza la confidencialidad, integridad y disponibilidad de la información en los servicios de

Hosting, Colocación, Respaldo y Almacenamiento Remoto, ofrecidos en los Data Center de Ciudad Universitaria (CUNI) y Santa Bárbara ubicados en Bogotá y Santa Mónica ubicado en Cali".

Para el Sistema de Gestión de Responsabilidad Social Corporativa el alcance de la Certificación es:

Implementación de una política de Responsabilidad Social Corporativa en los capítulos de:

- Relaciones Laborales: (Dialogo, Lugar para trabajar, Política de salud y seguridad en el trabajo)
- Relaciones con la sociedad: (Comunidad, Familia, clientes y proveedores)
- Responsabilidad con el medioambiente: Política medioambiental en favor de la comunidad)

Para el Sistema de Gestión Ambiental el alcance de la Certificación es:

"Planificación, diseño, comercialización, implementación, operación, mantenimiento, facturación, Tesorería y gestión en prestación de servicios de telecomunicaciones y de valor agregado para soluciones de transporte electrónico de datos, redes corporativas, canales dedicados, acceso a Internet e integración de soluciones en TIC´s en el ámbito local."

DEFINICIONES

Acción correctiva: Acción tomada para eliminar la causa de una no conformidad detectada u otra situación no deseable.

Acción preventiva: Acción tomada para eliminar la causa de una no conformidad potencial u otra situación potencial no deseable.

Alta dirección: Persona o grupo de personas que dirigen y controla una entidad al nivel más alto.

Arquitectura empresarial: La organización fundamental de un sistema, representada por sus componentes, sus relaciones entre ellos y con su entorno, y los principios que gobiernan su diseño y evolución.

Aspecto ambiental: Elemento de las actividades, productos o servicios de una entidad que puede interactuar con el medio ambiente.

Auditoría: proceso sistemático, independiente y documentado para obtener evidencias de la auditoría y evaluarlas de manera objetiva con el fin de determinar la

extensión en que se cumplen los criterios de auditoría[1]. Pueden ser de primera, segunda o tercera parte (Internas, externas y a los proveedores).

Cliente: entidad o miembro individual del público general que compra propiedad, productos o servicios para propósitos comerciales, privados o públicos.

Comité: Es un grupo de trabajo que con arreglo a las leyes o reglas de una organización, institución o entidad tienen establecidas determinadas competencias en áreas específicas.

Competencia: atributos personales y aptitud demostrados para aplicar conocimientos y habilidades.

Confidencialidad: Propiedad de que esa información esté disponible y no sea divulgada a personas, entidades o procesos no-autorizados (ISO/IEC 13335-1:2004).

Conservación: Procesos y operaciones realizados para garantizar la permanencia intelectual y técnica de documentos auténticos a lo largo del tiempo.

Continuidad del negocio: Capacidad estratégica, táctica y operativa de la entidad para planificar y responder ante incidentes e interrupciones del negocio para continuar las operaciones de negocio en un nivel aceptable predefinido.

Declaración de aplicabilidad: Documento que describe los objetivos de control y los controles que son relevantes y aplicables al SGSI de la entidad.

Desarrollo sostenible: Desarrollo que satisface las necesidades del presente sin comprometer la capacidad de las generaciones futuras para satisfacer sus propias necesidades.

Disposición: Decisión resultante de la valoración hecha en cualquier etapa del ciclo vital de los documentos, registrada en las tablas de retención y/o tablas de valoración documental, con miras a su conservación total, eliminación, selección y/o reproducción.

Documento: Información y su medio de soporte. Información u objeto registrado que puede ser tratado como una unidad.

Dominio: Es un conjunto sistemático de procesos de negocio agrupados e interrelacionados de forma lógica y estructurada con el fin de alcanzar un objetivo común, logrando objetivos estratégicos de la compañía y la promesa de valor al cliente.

[1] Norma Internacional ISO 19011. Directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiental. ISO, Suiza, 2002.

Dueño de proceso: persona responsable de gestionar el proceso.

Estructura organizacional: Es el conjunto de los cargos de una entidad y de las relaciones jerárquicas entre estos. Es una estructura intencional de roles, cada persona asume un papel que se espera que cumpla con el mayor rendimiento posible.

Factor crítico de éxito: Son componentes o elementos constitutivos clave de una entidad, transformados en variables, donde sus valores pueden afectar críticamente un proceso, producto u entidad.

Gestión del conocimiento: La gestión del conocimiento es el proceso que continuamente asegura el desarrollo y la aplicación de todo tipo de conocimientos pertinentes de una empresa con objeto de mejorar su capacidad de resolución de problemas y así contribuir a la sostenibilidad de sus ventajas competitivas (Andreu & Sieber 1999).

Gobierno: Es el conjunto de roles, responsabilidades y atribuciones de los órganos directivos, que direccionan los intereses de la Entidad.

Grupos de Interés: Individuo o grupo que tiene interés en cualquier decisión o actividad de la entidad.

Impacto ambiental: Efecto que produce la actividad humana (corporativa) sobre el medio ambiente.

Mejora continua: Acción permanente realizada, con el fin de aumentar la capacidad para cumplir los requisitos y optimizar el desempeño.

Metodología: Hace referencia a un conjunto de procedimientos utilizados para alcanzar unos objetivos o tareas que requieren habilidades, conocimientos o cuidados específicos.

Modelo: Es un esquema teórico, de un sistema o realidad compleja, que se elabora para facilitar su comprensión y el estudio de su comportamiento[2].

Normograma: Instrumento que le permite a las entidades delimitar su ámbito de responsabilidad, tener un panorama claro sobre la vigencia de las normas que regulan sus actuaciones, evidenciar las relaciones que tiene con otras entidades en el desarrollo de su gestión, identificar posible duplicidad de funciones o responsabilidades con otros entes públicos y soportar sus planes, programas, procesos, productos y Servicios.

Recursos: La totalidad de activos, personas, habilidades, información, tecnología (incluyendo planta y equipo) premisas y suministros e información (ya sea electrónica

[2] Diccionario de la real academia Española. Vigésima segunda edición. España, 2001.

o no) que una entidad debe tener disponible para uso, cuando se necesite para operar y cumplir con sus objetivos.

Registro: Documento que presenta resultados obtenidos o proporciona evidencia de actividades desempeñadas.

Satisfacción del cliente: Grado de conformidad del usuario o comprador con el producto adquirido o el servicio recibido.

CONTEXTO

Empresa de Telecomunicaciones de Bogotá

La Empresa de Telecomunicaciones de Bogotá S.A. – E.S.P (ETB), fundada en 1884 es una compañía líder del sector de las telecomunicaciones de Colombia que brinda servicios de telefonía local, móvil, larga distancia, Internet, datos y TV a clientes de hogares, pymes, grandes empresas y Gobierno consolidándose como una empresa sólida que contribuye al crecimiento del país, generando empleo y siendo soporte para el desarrollo de la industria y el comercio.

Valores Corporativos

Excelencia:

Nuestra motivación es trabajar impulsados a ser mejores cada día; esfuerzo que demanda calidad, empeño y coraje con el fin de trascender la experiencia de nuestros clientes y usuarios.

Integridad:

Nuestro compromiso es actuar con transparencia y coherencia, para generar confianza con todos nuestros grupos de interés.

Pasión por el Cliente:
Nuestra inspiración son nuestros clientes y usuarios, por ello, trabajamos día a día por brindarles la mejor experiencia.

Composición del Sistema Integrado de Gestión

El Sistema Integrado de Gestión de ETB, se encuentra conformado por ocho Sistemas de Gestión, los cuales se relacionan a continuación:

Sistema de Gestión de Calidad

Desde el año 2000 la organización ha venido construyendo un Sistema de Gestión de Calidad siguiendo los requisitos de la norma ISO 9001. Durante este tiempo ha evolucionado en el entendimiento de la importancia de la gestión por procesos, la satisfacción del cliente y el mejoramiento continuo, concluyendo que sobre éstos se edifica la calidad. Es por esta razón que ETB ha emprendido el camino de certificar su sistema de gestión y utilizarlo como piedra angular de la integración, armonizando los diferentes sistemas de gestión dentro de lo que hoy conocemos como Sistema Integrado de Gestión.

El Sistema Integrado de Gestión busca que ETB cuente con una herramienta de gestión que le permita dirigir y evaluar el desempeño institucional, en términos de calidad y satisfacción de las partes interesadas en la prestación de sus servicios.

Sistema de Gestión Ambiental

En el año 2005, la Empresa de Telecomunicaciones de Bogotá ETB S.A., como empresa socialmente responsable con el Medio Ambiente, se adhirió al Pacto Mundial Global, a través de la iniciativa que promovió la Asociación Nacional de Empresas de Servicios Públicos y Comunicaciones Andesco, e integró a sus prácticas empresariales el Séptimo Objetivo del Milenio asociado a garantizar la sostenibilidad del medio ambiente, cuya meta principal es propender por la reducción del agotamiento de los recursos naturales y la degradación de la calidad del medio ambiente.

En ese sentido, ETB conformó el Equipo de Gestión Ambiental en la Gerencia de Bienestar y Seguridad Industrial de la Vicepresidencia de Gestión Humana; y en el año 2006 concertó el Plan Institucional de Gestión Ambiental -PIGA-.

Este documento enmarca la gestión ambiental de la Compañía, su estructura sigue los lineamientos de la NTC ISO 14001:2004, establece el Sistema de Gestión Ambiental SGA, y busca promover acciones para el uso racional de los recursos naturales y aportar a un ambiente sano para la ciudad, a través de prácticas que contribuyan al cumplimiento de objetivos específicos del Plan de Gestión Ambiental Distrital; el desarrollo de actividades destinadas a prevenir, mitigar, corregir o compensar los

impactos negativos y potenciar los impactos positivos; y el compromiso de nuestros trabajadores y contratistas con el uso de mejores prácticas para el cuidado del medio ambiente en torno a los proyectos y servicios de telecomunicaciones que la entidad desarrolla a diario.

En cumplimiento del Decreto 243 del 18 de Junio de 2009, se designó al Vicepresidente de Gestión Humana, en julio de 2010, como el Gestor Ambiental y representante ante la alta dirección del Sistema de Gestión Ambiental (SGA); así mismo, en diciembre del mismo año, se creó el Comité del Plan Institucional de Gestión Ambiental –COPIGA–, para garantizar una efectiva y armónica implementación y seguimiento del PIGA.

Algunos beneficios que la entidad obtiene al implementar el Sistema de Gestión Ambiental enmarcado en el PIGA son:

- Mejoramiento del desempeño ambiental, de la imagen de la entidad y de las relaciones con partes interesadas;
- Divulgación del compromiso ambiental de la entidad;
- Permite el acceso a capital y a mercados nuevos y existentes;
- Obtención de seguros a costos razonables;
- Facilita el control de costos, optimizando procesos y racionalizando el uso de los recursos;
- Ayuda a lograr y mantener el cumplimiento legal;
- Reduce riesgos ambientales;
- Estimula actitud más responsable de los empleados frente al medio ambiente.

Sistema de Gestión de Riesgos

El sistema de gestión de riesgos tiene como objetivo orientar a las áreas en la identificación y valoración correcta y oportuna de los riesgos y sus planes de tratamiento, para controlar y mitigar el impacto de los mismos enfocándose en crear y proteger el valor ya que contribuye tanto logro de los objetivos como a la mejora del desempeño empresariales siendo una herramienta para la toma de decisiones y un facilitador de la mejora continua de la entidad.

En concordancia con las estrategias que ha venido desarrollando la Presidencia a fin de garantizar el cumplimiento de los estándares de Buen Gobierno adoptados por la compañía y generar valor al negocio se definió el apetito del riesgo como el nivel de exposición al riesgo que la entidad está dispuesta a aceptar, así como la unificación de la metodología corporativa para la administración de riesgos, la cual debe ser

implementada activamente por toda la entidad, de igual manera, a funciones y proyectos específicos siguiendo las políticas y directrices que en ésta se impartan de una manera sistémica, transparente y confiable, y en alcances y contextos concretos.

Esta metodología está regulada por la Directiva Interna No. 645 a la cual se puede acceder a través de Intrared.

Para identificar, evaluar y tratar los riesgos a procesos, ETB ha diseñado el proceso llamado Gestión de riesgos, el cual apoya la metodología corporativa.

Sistema de Gestión de Seguridad de la Información

El SGSI, establece un marco de trabajo que refleja el enfoque de ETB hacia la gestión del riesgo, los objetivos de control, sus controles correspondientes y el grado de confianza requerido. El SGSI establece un sistema de gestión basándose en los tres pilares de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad. Así mismo, con la implantación de SGSI se establece en resumen un aumento de la seguridad en base a la mejora de procesos y al conocimiento interno de las reglas para poder manejar la información, reducción de los costos de tales procesos y un aumento de la seguridad en base a la gestión de procesos.

Sistema de Gestión de Responsabilidad Corporativa

El Sistema de Responsabilidad Corporativa en ETB es un conjunto de prácticas, implementadas en el marco de la guía de responsabilidad social ISO 26000:2010, que integran la gobernanza de la entidad, la identificación de los impactos de las operaciones de la compañía, el compromiso con los grupos de interés y la aplicación de los Principios del Pacto Mundial en la gestión empresarial, a través de la implementación de programas orientados al desarrollo sostenible y la promoción en la ciudadanía del acceso, uso y apropiación de las TIC, como herramienta de desarrollo e inclusión.

Sistema de Gestión de Continuidad del Negocio

La estructura de continuidad del negocio en ETB está conformada por tres niveles.

Estratégico: Basado en el comité de manejo de crisis desde donde se encaran las cuestiones estratégicas de la crisis y se ejerce control sobre las actividades relevantes de los niveles táctico y operativo.

Táctico: Basado en el comité de continuidad del negocio, desde donde se movilizan y gestionan los recursos alternos necesarios para la recuperación, se coordina la respuesta con actores externos y se hace seguimiento y control al nivel operativo; todo aquello que supere el alcance de este nivel, debe ser escalado al nivel estratégico.

Operativo: Basado en los planes de respuesta de incidentes y reinicio de actividades, es decir donde se ejecutan las actividades en pro del reinicio de las funciones normales del negocio a nivel de las operaciones; este nivel reporta al táctico y es a quien escala todo aquello que supere su alcance.

El nivel estratégico responde a la eventualidad de crisis presentadas en la entidad en general, mientras que los niveles táctico y operativo tienen en su alcance actual la infraestructura tecnológica con que la entidad soporta los servicios de cara al cliente externo.

Sistema de Gestión de Seguridad y Salud en el Trabajo

Es motivo de interés para ETB la identificación, análisis y evaluación de los riesgos ocupacionales que puedan afectar a los trabajadores, o que puedan producir daños sobre los equipos, herramientas, materiales o interferencias sobre el proceso o el servicio, por esta razón se diseñaron estrategias encaminadas a minimizar y controlar los riesgos identificados.

La implementación del programa de Salud Ocupacional se constituye en una herramienta para la planeación y ejecución de actividades tendientes a mejorar la salud de los trabajadores y buscar el máximo de bienestar de las personas en su ambiente de trabajo, en procura de dar mayor alcance a las actividades orientadas al control de los riesgos en el trabajo, ETB trabaja en la implantación y aseguramiento de un sistema de Gestión en Seguridad Industrial y Salud Ocupacional, bajo los parámetros de la norma OHSAS 18001; ésta norma internacional establece un conjunto de requisitos relacionados con los sistemas de gestión de la Seguridad y Salud en el trabajo y permite controlar los riesgos laborales y mejorar el rendimiento en materia de Seguridad y Salud. De esta manera ETB fomenta la cultura preventiva, genera capacidad de identificar, evaluar y controlar los riesgos asociados a cada lugar, propende por unas condiciones de trabajo más seguras que redundan en aumento de la productividad. La empresa también obtendrá mejora en la percepción de las partes interesadas en relación con la Gestión de Seguridad en el trabajo.

Sistema de Gestión Documental

El Sistema de Gestión Documental, establece los parámetros básicos que se deben tener en cuenta para la administración adecuada de los documentos, los cuales incluyen (producción, recepción, distribución, trámite, entidad, consulta, conservación y

disposición final), procedimientos que se ajustan a las necesidades propias para el manejo de la información y la documentación, basados en términos de calidad y todo enmarcado en el ciclo vital de los documentos.

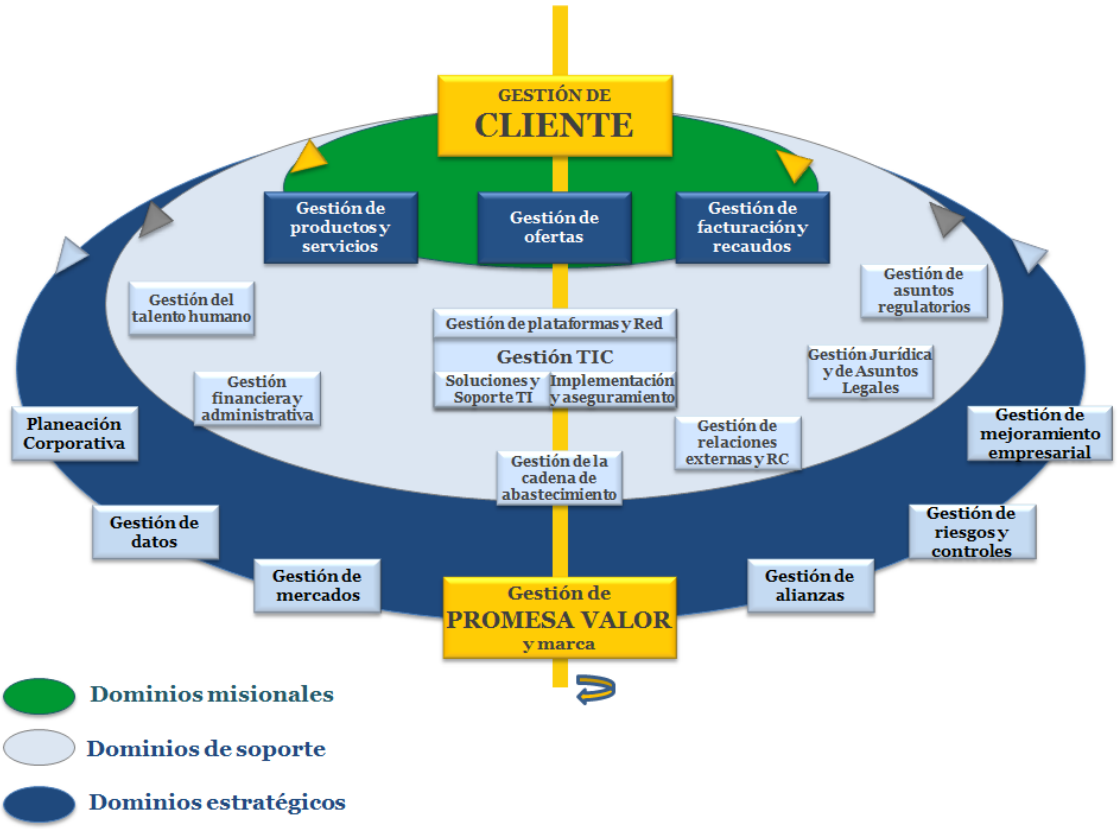
NORMAS Y DOCUMENTOS DE REFERENCIA

ETB para el desarrollo del Sistema Integrado de Gestión aplica la Norma Integrada de Gestión (Norma SIG), la cual integra los requisitos de las siguientes normas:

- Norma ISO 9001:2008 y NTCGP 1000:2009 - Sistema de Gestión de Calidad
- Norma OHSAS 18001: 2007- Sistema de Gestión de Seguridad Industrial y Salud Ocupacional
- Norma ISO 14001:2004- Sistema de Gestión Ambiental
- Norma ISO 31000:2011- Sistema de Gestión de Riesgos
- Guía ISO 26000:2010 y Principios del Pacto Mundial- Sistema de Gestión de Responsabilidad Corporativa
- Norma NTC 31301:2013- Sistema de Gestión Documental
- Norma ISO 22301:2012 - Sistema de Gestión de Continuidad del Negocio
- Norma ISO 27001:2013- Sistema de Gestión de Seguridad de la Información

Y todas aquellas otras normas, resoluciones, decretos, entre otros, aplicables a la entidad.

MAPA DE PROCESOS ETB



Descripción del Mapa de Procesos

El mapa de procesos ETB está basado en la metodología de dominios, que le permite a la entidad identificar fácilmente la agrupación de todos los procesos requeridos para el funcionamiento de la entidad. Los dominios definidos para ETB, se encuentran divididos en tres niveles, los cuales se clasifican de acuerdo a la importancia frente al modelo operativo:

Estratégicos y corporativos: Conjunto de procesos a través de los cuales una entidad pública, gerencia el diseño y desarrollo de los demás procesos.

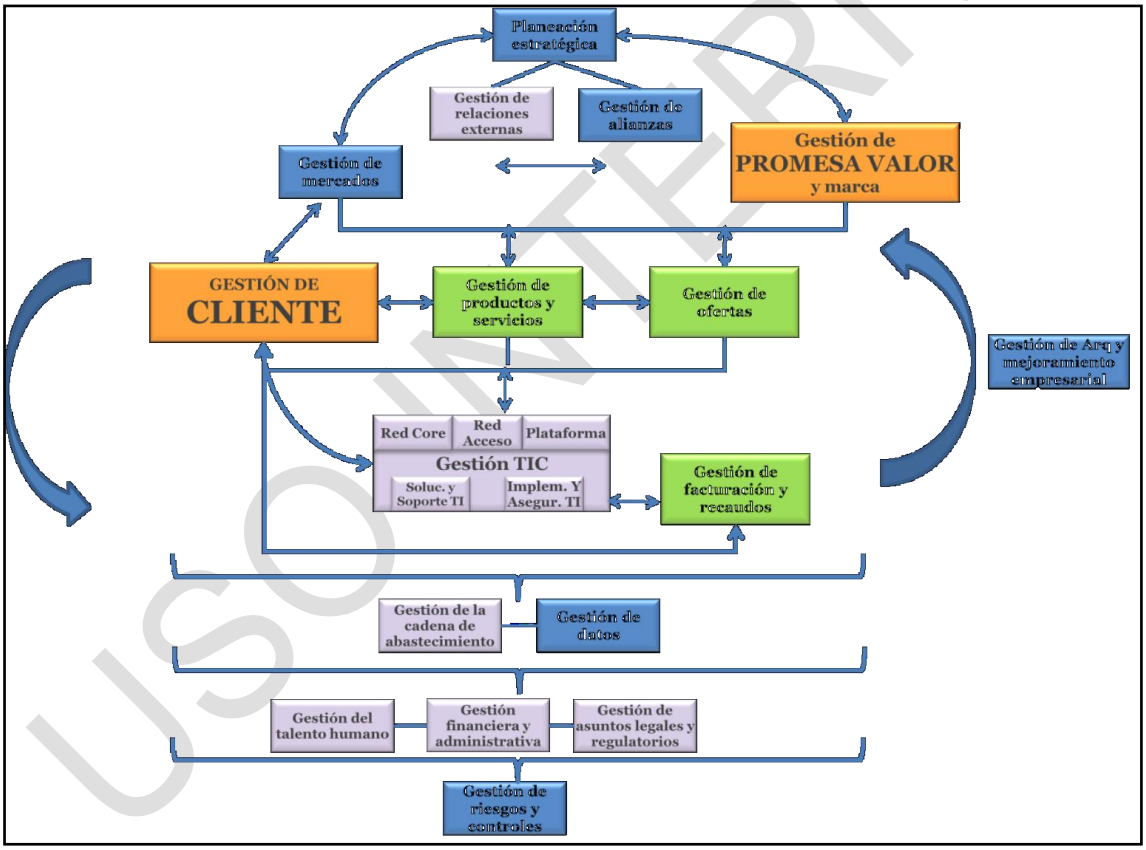
Soporte: Corresponde al conjunto de procesos que no se relacionan de forma directa con la creación de productos y/o servicios propios del ejercicio y la misión de ETB, estos dominios dan soporte a los niveles misionales y estratégicos para dar continuidad a su desarrollo.

Misionales: Entendidos como el conjunto de procesos y actividades estratégicas y relevantes para la entidad que se relacionan de forma directa con la razón de ser de la empresa, misión organizacional, generación de resultados, venta de productos o servicios y relacionamiento con cliente.

Interrelación de los dominios

En la siguiente figura se muestra gráficamente como se interrelacionan los dominios de ETB.

Este gráfico se realiza para dar a entender de manera general, cómo funciona el ciclo de operación de la entidad según el mapa de procesos.



La interrelación de los dominios comienza desde la planificación estratégica, donde se dan los lineamientos y políticas corporativas para la gestión en la entidad; adicionalmente se planifican las estrategias de responsabilidad corporativa y las alianzas requeridas para el desarrollo de los planes.

Cuando los lineamientos de la entidad están definidos, se realiza la gestión de mercados, que a su vez proporciona elementos para mejorar la planificación estratégica y para definir la promesa de valor y operar con base en ésta.

La gestión de mercados identifica los diferentes segmentos de clientes a los que la entidad ofrecerá sus productos y servicios y las ofertas que puede hacerles.

Luego que en los dominios anteriores realizan las actividades de mercadeo, ventas, conocimiento del cliente, segmentación; continúa la prestación del servicio, la cual está en los procesos del dominio de gestión de TIC.

Después de prestado el servicio se procede a la facturación, que se encuentra en el dominio de gestión de cliente, el cual genera entradas para la gestión de clientes y de mercados donde se realiza la medición de la satisfacción y la adecuación de los servicios de acuerdo con las necesidades de los mismos, proporcionando nuevos elementos para la mejora y posibles cambios dentro de la planificación, la promesa de valor, las ofertas, generar nuevas alianzas y fortalecer las relaciones externas.

Por otra parte, para realizar la operación con éxito, existen unos procesos que son transversales y se deben realizar paralelamente con los demás. En primer lugar se encuentra el dominio de cadena de abastecimiento, que soporta a la operación desde la gestión de los proveedores, inventarios y logística. Por otra parte están la gestión de información, la cual es necesaria para mantener la información de la entidad; a través de este dominio se controla, protege, recupera, se mantiene la integralidad, la distribución, el acceso y la seguridad de los datos, que se generan en toda la operación, incluidos los datos de los clientes.

Desde los dominios de talento humano y recursos administrativos y financieros se realiza la provisión de los recursos para la operación, prestación del servicio y mejora de la entidad. Adicionalmente se controla la documentación de ETB como base para la toma de decisiones y blindaje legal.

Como un proceso transversal a toda la entidad, el cual soporta el cumplimiento de sus objetivos se encuentra el dominio de riesgos y controles el cual genera lineamientos para todos los dominios en materia de identificación, análisis, evaluación y tratamiento de los riesgos y, por otra parte recibe de los demás dominios la información sobre los riesgos a los que está expuesta la entidad, para determinar dentro de la planeación corporativa el criterio, el apetito, la tolerancia y demás políticas que deben definirse desde la planificación para la gestión de los riesgos en la entidad. Por otra parte proporciona los procesos necesarios para la realización de las auditorías del SIG y de control interno de la entidad.

Finalmente se encuentra el dominio de mejoramiento empresarial, que recibe entradas de los demás para el establecimiento, implementación, mantenimiento y monitoreo de

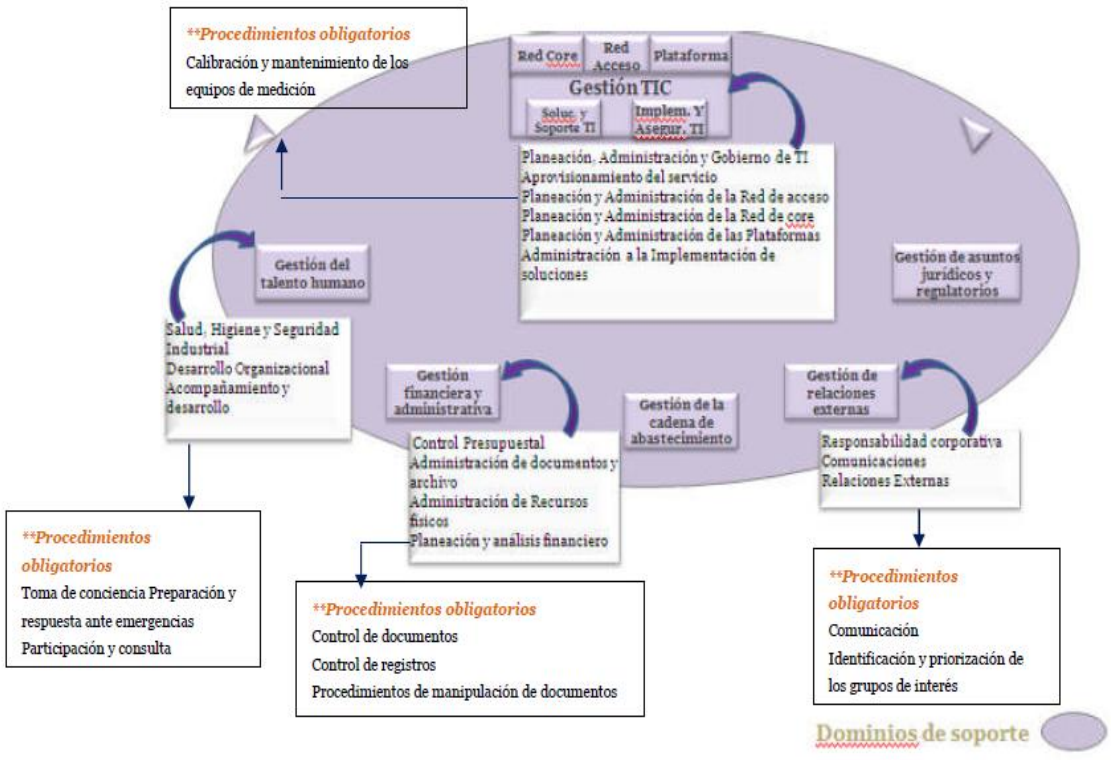
planes de mejora y a su vez los entrega a cada uno de los dominios del mapa de procesos; por otra parte establece los lineamientos de la gestión por procesos, y de la arquitectura empresarial, ambas como base de la gestión de la entidad.

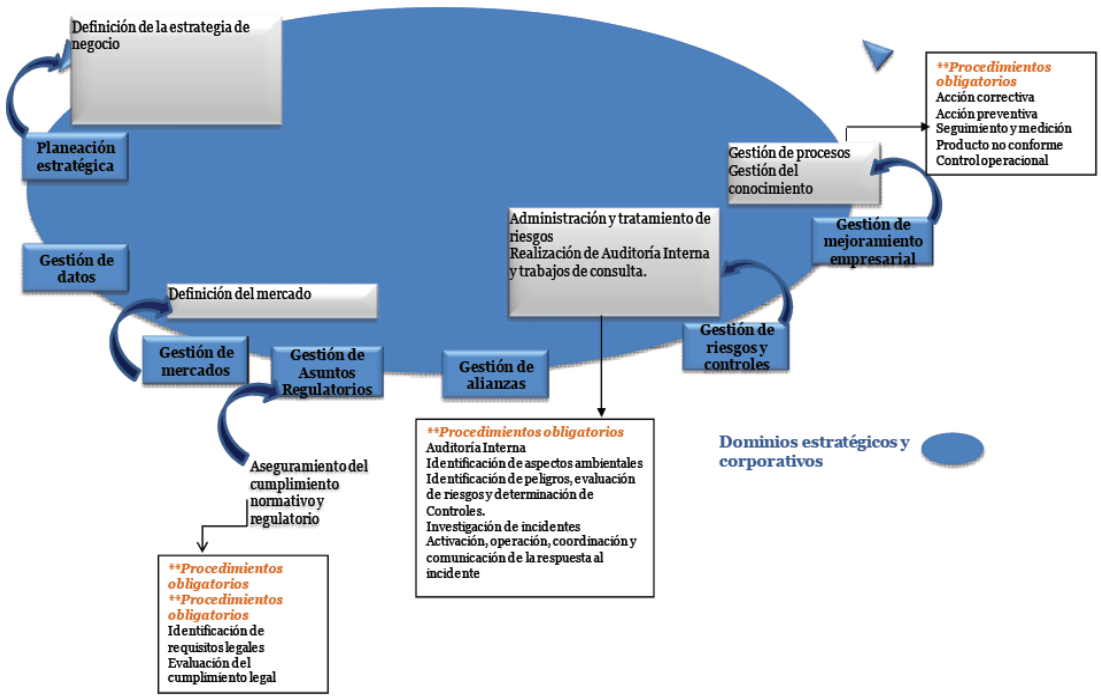
MAPA DE PROCESOS SIG

Para cada uno de los elementos integradores del sistema de gestión se realiza una alineación con los dominios del modelo operativo que establece el cumplimiento de los requisitos del SIG en los procesos de ETB, para que estén inmersos en el día a día de la operación y no sea una carga adicional para la entidad.

A continuación se presentan los dominios con los procesos que dan cumplimiento a los elementos integradores del SIG y se identifican los procedimientos documentados obligatorios.

Los procedimientos mandatorios se encuentran ubicados en ADONIS.





Tomado de: Documento Modelo del Sistema Integrado de Gestión –PWC (Fase 7-3.2.2) .2012-03.26. GDE- VPEN

MODELO DEL SISTEMA INTEGRADO DE GESTIÓN

El modelo de gestión del SIG de ETB, tiene como finalidad apoyar a la entidad en la mejora continua y buscar la excelencia en cada una de sus actividades, a través de la interrelación de sus componentes.

OBJETIVOS DEL SISTEMA INTEGRADO DE GESTIÓN

Objetivo General

Contribuir al logro de los objetivos de ETB y a la identificación, cumplimiento y la satisfacción de los requisitos de sus grupos de interés, facilitando la toma de decisiones, a través de la gestión integrada de los sistemas de gestión, potencializando las interrelaciones existentes por medio de elementos integradores

como: la gestión documental, la disponibilidad de los recursos, la gestión de los riesgos y aplicación de controles, la planificación del servicio, el seguimiento de los procesos, el desarrollo integral de su talento humano, la comunicación, y el modelo que los soporta; buscando la excelencia con el compromiso de la mejora continua para prestar un servicio permanente de calidad, que contribuya al desarrollo sostenible.

Objetivos Específicos

El Sistema Integrado de Gestión adopta los direccionadores (austeridad, rentabilidad y servicio al cliente) como objetivos específicos y desarrolla los siguientes objetivos de manera particular pero en alineación con direccionadores:

- Cumplir los requisitos legales aplicables
- Mantener y mejorar el desempeño ambiental

Para conocer los retos estratégicos, puede hacerlo a través de la Intrared Corporativa siguiendo la siguiente ruta https://intranet.etb.com.co/ .

EXCLUSIONES

El Sistema Integrado de Gestión de ETB tiene exclusiones sobre los requisitos establecidos por la norma NTC-ISO/IEC 27001:2013 las cuales se establecen en el documento “Declaración de Aplicabilidad - SOA” , Anexo A de este documento, donde se referencian los controles, objetivos de los controles que han sido seleccionados y los controles excluidos.

POLÍTICA DEL SIG

En ETB desarrollamos un portafolio de servicios de telecomunicaciones que agregan valor, basado en el entendimiento y satisfacción de los grupos de interés a partir del autocontrol y mejoramiento continuo, buscando la eficacia, eficiencia y efectividad de sus procesos, fomentando una gestión social, ambiental y económicamente responsable, ética y transparente.

ETB está comprometida con el cumplimiento de los requisitos legales, estándares e iniciativas mundiales, nacionales y locales aplicables , mediante la gestión de riesgos, la prevención de lesiones, accidentes de trabajo y enfermedades profesionales, la

prevención de la contaminación y mitigación de los impactos ambientales significativos, la continuidad del negocio, la seguridad de la información, la gestión documental y las acciones que voluntariamente ha asumido con la comunidad y sus zonas de influencia, lo que le permite posicionarse como una empresa competitiva y con un alto compromiso con el desarrollo sostenible y tecnológico del país, garantizando los recursos humanos competentes y tecnología adecuada para el logro de los objetivos trazados para la organización.

CONTROL DE DOCUMENTOS Y REGISTROS

ETB cuenta con el Procedimiento de Control de Documentos y Registros, el Manual de Control de Documentos y Registros, el Instructivo de Estandarización Documental y el Instructivo de Codificación y Versionamiento, documentos que describen la estructura documental de ETB y despliegan los lineamientos que en esta materia deben ser cumplidos en todos los procesos de la entidad.

AUDITORÍAS A SISTEMAS DE GESTIÓN

El Sistema Integrado de Gestión cuenta con el procedimiento de Auditorías a Sistemas de Gestión, el cual define el paso a paso de las actividades de auditoría y diagnóstico de los sistemas que componen el SIG.

REPRESENTANTE POR LA DIRECCIÓN

La presidencia de ETB comprometida con una implementación eficiente del SIG en la compañía, ha dispuesto de recursos financieros y humanos para apoyar la operación y asegurar el seguimiento y mejora continua de la gestión corporativa.

Por lo cual ha designado a los vicepresidentes de ETB la función de ser representantes de la dirección teniendo en cuenta los sistemas de gestión que sus áreas funcionales soportan.

REVISIÓN POR LA DIRECCIÓN

En el gobierno del Sistema integrado de Gestión se definen dos tipos de comité los cuales permiten realizar articulación y seguimiento a las acciones que conjuntamente entre los sistemas se han establecidos como parte de la implementación,

sostenimiento de los sistemas de gestión que componen el SIG. Así mismo estos espacios permiten el cumplimiento de aspectos legales en los cuales ETB requiere el concurso de la alta dirección.

Comités Y Composición

Comité directivo: Compuesto por los representantes por la dirección o sus delegados, espacio en el cual se presentan los resultados y avances de los sistemas, y se gestionan aspectos que requieren el concurso de la alta dirección para su movilización o validación. Este comité se convoca y reúne a demanda con un mínimo de una vez al año.

Comité táctico: Compuesto por los líderes de los sistemas de gestión, es un espacio donde se realiza seguimiento a los planes de acción de cada uno de los sistemas y se articulan acciones en pro de la mejora y el sostenimiento de los sistemas. Este comité sesiona a demanda con un mínimo de dos veces al año.

Roles Y Responsabilidades

Se establece dentro del gobierno del SIG, los siguientes roles y responsabilidades que permiten determinar la responsabilidad y autoridad de actores del SIG, teniendo en cuenta los requisitos particulares de cada uno de los sistemas y los generales al SIG.

Ver anexo Tabla de responsabilidades.

ANEXO A

(Normativo)

Los objetivos de control y controles listados se derivan directamente y están alineados con los requisitos de la norma ISO/IEC 27001:2013 Cor1:2014, del número 5 al 18, y están para ser usados en el contexto con la cláusula 6.1.3.

Tabla A.1 – Objetivos de control y controles

DECLARACION DE APLICABILIDAD – SOA				
SERVICIOS DE DATA CENTER (CUNI - SANTA BARBARA SANTA MONICA) Y OFICINA SEDE PRINCIPAL				
Código ISO	**Objetivo / Nombre ISO**	**Aplica (S/N)**	**Razón para la selección / Justificación para su exclusión**	**Control Actual / Documento Referencia**
A.5	**POLITICAS DE SEGURIDAD DE LA INFORMACION**			
A.5.1	Direccionamiento de la gestión de la seguridad de información	Proveer direccionamiento y soporte para la seguridad de la información de acuerdo con los requisitos del negocio y las leyes y regulaciones relevantes.		
A.5.1.1	Políticas para la seguridad de la información	SI	Se debe definir por la dirección las políticas para la seguridad de la información, para ser publicadas y divulgadas a las partes interesadas.	Documento de Políticas de Seguridad de la Información
A.5.1.2	Revisión de las políticas para la seguridad de la información	SI	Las políticas para la SI deben ser revisadas a intervalos planificados o si ocurren cambios asegurar su adecuación y eficacia.	Actas de validación y aprobación del Comité Empresarial de Seguridad de la Información de ETB
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION**			

A.6.1	Organización interna	Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información en la organización.		
A.6.1.1	Roles y responsabilidades de la seguridad de la información	SI	Se debe definir y asignar las responsabilidades de seguridad de la información	Documento de roles y responsabilidades de la Organización.
A.6.1.2	Segregación de tareas	SI	Las tareas y áreas con conflicto de responsabilidad deben ser segregadas para reducir las oportunidades de modificación no autorizada o el mal uso de los activos.	
A.6.1.3	Contacto con autoridades	SI	Se debe mantener contactos apropiados con las autoridades relevantes	ETB tiene convenios con la Policía Nacional, Red Papaz y con la CCIT - Cámara Colombiana de Informática y Telecomunicaciones.
A.6.1.4	Contacto con grupos especiales de interés	SI	Se debe mantener contacto apropiado con grupos especiales de interés así como otros foros especializados en seguridad de la información y asociaciones profesionales	ETB forma parte del Comité Técnico de Seguridad en NAP Colombia, Comunidad Internacional del FIRST – CSIRTs y el ColCERT.
A.6.1.5	Seguridad de la Información en gestión de proyectos	SI	La seguridad de la información debe ser considerada en la gestión de proyectos sin importar el tipo de proyecto	El manejo de la seguridad de la información está vinculado en la PMO de la Organización.
A.6.2	Dispositivos móviles y teletrabajo	Asegurar la seguridad del teletrabajo y el uso de dispositivos móviles		

A.6.2.1	Política para los dispositivos móviles	SI	Se debe adoptar una política y medidas de soporte para gestionar los riesgos introducidos por el uso de dispositivos móviles	Política de dispositivos móviles
A.6.2.2	Teletrabajo	SI	Se debe implementar una política y medidas de soporte para proteger la información accesada, procesada o almacenada en sitios de teletrabajo.	Política y medidas de soporte para proteger la información manejada en sitios de Teletrabajo
A.7	**SEGURIDAD EN LOS RECURSOS HUMANOS**			
A.7.1	Antes del empleo	Asegurar que trabajadores y contratistas entiendan sus responsabilidades y sean idóneos para los roles para los cuales son considerados.		
A.7.1.1	Verificación de antecedentes	SI	Debe realizarse la verificación de antecedentes para los candidatos conforme a las leyes y regulaciones relevantes, y la ética, de manera proporcional a los requisitos del negocio, la clasificación de la información a la cual tendrían acceso y los riesgos percibidos.	
A.7.1.2	Términos y condiciones para el empleo	SI	Los acuerdos contractuales con trabajadores y contratistas deben indicar las responsabilidades de ellos y de la organización en seguridad de la información.	Formato Contrato Contractual
A.7.2	Durante el empleo	Asegurar que trabajadores y contratistas son conscientes y cumplen con sus responsabilidades en seguridad de la		

		información.		
A.7.2.1	Responsabilidades de la dirección	SI	La dirección debe exigir que empleados y contratistas apliquen la seguridad de la información según las políticas y procedimientos de la organización.	Políticas Seguridad, Directiva Sistema de Gestión de Seguridad de la Información, Directiva Interna No 607 SGSI, Contratos de trabajo, procedimiento de Selección y contratación de personal, procedimiento de Formación y Desarrollo, Asignación de responsabilidades a funcionarios de ETB y terceros, Acuerdo de confidencialidad.
A.7.2.2	Toma de conciencia, educación y entrenamiento en seguridad de información	SI	Los empleados y contratistas deben recibir acciones de toma de conciencia, educación y entrenamiento, así como actualizaciones regulares en las políticas y procedimientos según sea relevante para su función y trabajo.	Plan de capacitación y entrenamiento empresarial
A.7.2.3	Proceso disciplinario	SI	Debe existir un proceso disciplinario formal y comunicado, para tomar acciones contra empleados que realicen rompimientos en la seguridad de la información.	
A7.3	Terminación o cambio en el empleo	Proteger los intereses de la organización en el proceso de cambio o finalización del empleo.		

A.7.3.1	Terminación o cambio en las responsabilidades del empleo	SI	Las responsabilidades y deberes que permanezcan válidas luego de terminar el empleo o ante su cambio, deben ser definidas, comunicadas al empleado o contratista.	Política Seguridad de Recursos Humanos, Check list o Paz y salvo de desvinculación, contratos de trabajo y prestación de servicios, acuerdos de confidencialidad.
A.8	**GESTION DE ACTIVOS**			
A.8.1	Inventario de activos	Identificar los activos organizacionales y definir las responsabilidades apropiadas de protección		
A.8.1.1	Inventario de activos	SI	Debe identificarse la información y otros activos asociados con la información y las instalaciones de procesamiento de información, y se debe realizar y mantener un inventario de activos.	Política Seguridad Física, Procedimiento Seguridad Física, normas de seguridad en zonas restringidas. Normas de seguridad con visitantes
A.8.1.2	Propiedad de los activos	SI	Los activos en el inventario deben tener un propietario.	Procedimiento de identificación, clasificación y valoración de activos de información.
A.8.1.3	Uso aceptables de los activos	SI	Se deben identificar, documentar e implementar reglas para el uso aceptable de la información y de los activos asociados con la información y las instalaciones de procesamiento de información.	

A.8.1.4	Devolución de activos	SI	Los empleados y usuarios de partes externas deben devolver los activos de ETB en su posesión al terminar su empleo, contrato o acuerdo.	
A.8.2	Clasificación de la información	Asegurar que la información recibe un nivel apropiado de protección según su importancia en la organización.		
A.8.2.1	Clasificación de la información	SI	La información debe clasificarse en términos de requisitos legales, valor, criticidad y sensibilidad a su divulgación o modificación no autorizada.	Instructivo para identificar, clasificar y valorar los activos de información
A.8.2.2	Etiquetado de la información	SI	Deben desarrollarse e implementarse un conjunto apropiado de procedimientos para el etiquetamiento de la información según los esquemas adoptados.	
A.8.2.3	Manejo de activos	SI	Se deben desarrollarse e implementar procedimientos para el manejo de activos de acuerdo con el esquema de clasificación de información adoptado.	
A.8.3	Manejo de Medios	Prevenir la divulgación, modificación, remoción o destrucción no autorizada de información almacenada en medios de almacenamiento.		
A.8.3.1	Gestión de medios removibles	SI	Deben implementarse procedimientos para la gestión de medios removibles de acuerdo con el esquema de	

			clasificación adoptado por la organización.	
A.8.3.2	Eliminación de medios	SI	Los medios deben eliminarse de forma segura, usando procedimientos formales, cuando ya no vayan a ser más utilizados.	Procedimiento de identificación, clasificación y valoración de activos de información.
A.9	**CONTROL DE ACCESO**			
A.9.1	Requisitos del negocio de control de acceso	Limitar el acceso a la información y a las instalaciones de procesamiento de información.		
A.9.1.1	Política de control de acceso	SI	Se debe establecer y documentar una política de control de acceso, la cual debe ser revisada según los requisitos del negocio y de la seguridad información	
A.9.1.2	Acceso a redes y servicios de red	SI	A los usuarios solo se les debe proveer acceso a la red y servicios de red a los cuales estén específicamente autorizados en su uso.	
A.9.2	Gestión de acceso de usuarios	Asegurar el acceso de usuarios autorizados y revenir el acceso no autorizado a sistemas y servicios.		
A.9.2.1	Registros y de-registro de usuarios	SI	Se debe implementar un proceso formal de registro de usuarios para permitir la asignación de derechos de usuarios	
A.9.2.2	Suministro de acceso a	SI	Se debe implementar un proceso formal de	

	usuarios		suministro de acceso a usuarios para asignar o revocar derechos de acceso para los tipos de usuarios a los sistemas y servicios.	
A.9.2.3	Gestión de derechos de acceso privilegiados	SI	Se debe restringir y controlar la asignación y uso de derechos de acceso de tipo privilegiado.	
A.9.2.4	Gestión de información secreta de autenticación de usuarios	SI	Se debe controlar la asignación de información secreta de autenticación a través de un proceso formal de gestión.	
A.9.2.5	Revisión de derecho de acceso de los usuarios	SI	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.	
A.9.2.6	Remoción o ajuste de derechos de acceso	SI	Se deben remover los derechos de acceso de los empleados y usuarios de partes externas, a la información así como instalaciones de procesamiento de la información, una vez terminada su vinculación, contrato o acuerdo, o ajustarse en cualquier cambio.	
A.9.3	Responsabilidades de los usuarios	Asignar responsabilidades a los usuarios respecto a la protección de su información de autenticación.		
A9.3.1	Uso de información secreta de autenticación	SI	Se debe requerir a los usuarios el seguir las prácticas de la organización sobre el	

			uso de la información secreta de la información.	
A.9.4	Control de acceso a sistemas y aplicaciones	Prevenir el acceso no autorizado a sistemas y aplicaciones		
A9.4.1	Restricción de acceso a la información	SI	Se debe restringir el acceso a la información y las funciones en las aplicaciones de acuerdo con la política de control de acceso	
A9.4.2	Procedimientos seguros de inicio de sesión	SI	Se debe controlar el acceso a los sistemas y aplicaciones por un procedimiento seguro de inicio de sesión, cuanto esto sea requerido por la política de control de acceso	
A9.4.3	Gestión de contraseñas	SI	Los sistemas de gestión de las contraseñas deben ser interactivos y asegurar contraseñas de calidad	
A.9.4.4	Uso de programas utilitarios privilegiados	SI	Deben estar restringido y controlado el uso de programas utilitarios que puedan ser capaces de evitar los controles del sistema y de las aplicaciones	
A.9.4.5	Control de acceso al código fuente de las aplicaciones	SI	Se debe restringir el acceso al código fuente de las aplicaciones	
A.10	**CRIPTOGRAFIA**			

A.10.1.1	Controles criptográficos	Asegurar el uso adecuado y eficaz de cifrado para proteger la confidencialidad, la autenticidad y/o la integridad de la información.		
A.10.1.1	Política de uso de controles criptográficos	SI	Se debe desarrollar e implementar una política para el uso de controles criptográficos para la protección información.	
A.10.1.2	Gestión de claves	SI	Se debe desarrollar e implementar una política para el uso, protección y gestión del ciclo de vida de las claves del cifrado.	
A.11	**SEGURIDAD FISICA Y AMBIENTAL**			
A.11.1	Áreas seguras	Prevenir el acceso físico no autorizado al igual que el daño e interferencia a la información e instalaciones de procesamiento de información de la organización.		
A.11.1.1	Perímetro de seguridad física	SI	Se deben definir y usar perímetros de seguridad física para proteger áreas que contengan información crítica o sensible, o instalaciones de procesamiento de información.	
A.11.1.2	Controles físicos de entrada	SI	Las áreas seguras deben estar protegidas por controles de entrada apropiados para asegurar que solo se permite acceso al personal autorizado.	
A.11.1.3	Aseguramiento de oficinas, áreas e instalaciones	SI	Se debe diseñar y aplicar seguridad física para oficinas, áreas e instalaciones.	
A.11.1.4	Protección contra	SI	Se debe diseñar y aplicar protección física	

	amenazas externas ambientales		contra desastres naturales, ataques maliciosos o accidentes.	
A.11.1.5	Trabajo en áreas seguras	SI	Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.	
A.11.1.6	Áreas de entrega y carga	SI	Se deben controlar, y aislar de las instalaciones de procesamiento de datos, aquellos puntos de acceso tales como áreas de entrega y de carga así como aquellos otros puntos donde el personal no autorizado pudiese ingresar al recinto, con el fin de evitar acceso no autorizado.	
A.11.2	Equipos	Prevenir la pérdida, daño, robo o compromiso de activos y la interrupción de las operaciones de la organización		
A.11.2.1	Emplazamiento y protección de equipos	SI	Los equipos deben estar emplazados y protegidos para reducir los riesgos de amenaza ambiental y peligros, así como la oportunidad de acceso no autorizado.	
A.11.2.2	Servicios de soporte	SI	Los equipos deben estar protegidos de fallas eléctricas y otras disrupciones y causadas por fallas en los servicios de soporte.	
A.11.2.3	Seguridad del cableado	SI	Se debe proteger de interceptación, interferencia o daño, el cableado de energía y telecomunicaciones que	

			transporte datos o soporte de los servicios.	
A.11.2.4	Mantenimiento de equipos	SI	Los equipos deben recibir mantenimiento adecuado para garantizar disponibilidad e integridad continuadas	
A.11.2.5	Remoción de activos	SI	No debe retirarse equipos, información o software, de su sitio, sin autorización.	
A.11.2.6	Seguridad de equipos y activos fuera de su sitio	SI	Se debe aplicar seguridad a los activos fuera de su sitio de emplazamiento considerando los riesgos para los trabajos fuera de las áreas de la organización.	
A.11.2.7	Eliminación segura o re-uso de equipos	SI	Los elementos de los equipos que contengan medios de almacenamiento deben ser verificados para asegurar que los datos sensibles y el software con licencia hayan sido removidos de manera segura antes de su eliminación o reúso.	
A.11.2.8	Equipo de usuario desatendido	SI	Los usuarios deben asegurar que los equipos desatendidos tengan protección adecuada.	
A.11.2.9	Política de escritorio limpio	SI	Se debe adoptar una política para escritorio limpio aplicado a documentos y medios de almacenamiento removibles así como una política de pantalla	

			limpia para instalaciones de procesamiento de información.	
A.12	**SEGURIDAD EN LAS OPERACIONES**			
A.12.1	Procedimientos y responsa-bilidades operacionales	Asegurar la operación segura y correcta de las instalaciones de procesamiento de información		
A.12.1.1	Procedimientos operativos documentados	SI	Los procedimientos operativos deben estar documentados y disponibles a los usuarios que los necesiten	
A.12.1.2	Gestión del cambio	SI	Se deben controlar los cambios a la organización, a los procesos de negocio, a las instalaciones de procesamiento de información y a los sistemas que afecten la seguridad información.	
A.12.1.3	Gestión de la capacidad	SI	Se debe monitorear y optimizar el uso de recursos y realizar proyecciones sobre futuros requisitos de capacidad para asegurar el desempeño requerido.	
A.12.1.4	Separación de ambientes de prueba y de producción	SI	Los ambientes de desarrollo, pruebas y producción deben estar separados para reducir los riesgos de acceso no autorizado o cambios al ambiente de producción.	

A.12.2	Protección contra malware	Asegurar que la información y las instalaciones de procesamiento de información se protegen contra malware.		
A.12.2.1	Controles contra malware	SI	Se debe implementar controles de detección, prevención y recuperación contra malware, en combinación con la toma de conciencia adecuada en los usuarios.	
A.12.3	Back-up (Copia de Respaldo)	Proteger contra pérdidas de datos		
A.12.3.1	Back-up (copia de respaldo) de la información.	SI	Se deben realizar copias de seguridad de la información del software así como imágenes de los sistemas y ser probadas según la política de copia de respaldo.	
A.12.4	Registro y supervisor	Registrar eventos y generar evidencia		
A.12.4.1	Registro de eventos	SI	Se deben producir, mantener y revisar regularmente los registros de eventos de actividad del usuario, excepciones y de seguridad información.	
A.12.4.2	Protección de la información del registro	SI	Las instalaciones de registro y la información de registro deben estar protegidas contra manipulación y acceso no autorizado.	
A.12.4.3	Registros de administrador y del operador	SI	Las actividades del administrador del sistema así como del operador del sistema	

			deben estar registrados y estos registros protegidos y revisados de manera regular.	
A.12.4.4	Sincronización de relojes	SI	Los relojes de los sistemas relevantes del procesamiento de información dentro de una organización deben estar sincronizados a una única fuente de referencia de tiempo.	
A.12.5	Control de Software para producción	Asegurar la integridad de los sistemas en producción.		
A.12.5.1	Instalación de Software en sistemas de producción	SI	Se deben implementar procedimientos para controlar la instalación de software en sistemas operacionales.	
A.12.6	Gestión de vulnerabilidades técnicas	Prevenir la explotación de las vulnerabilidades técnicas		
A.12.6.1	Gestión de vulnerabilidades Técnicas	SI	Se debe obtener de manera oportuna información sobre vulnerabilidades técnicas de los SI, así como de la exposición de la organización	
A.12.6.2	Restricciones en la instalación de software	SI	Se deben establecer e implementar reglas para instalación de software por parte de usuarios.	
A.12.7	Consideraciones de auditoría de sistemas de información	Minimizar el impacto de las actividades de auditoría en sistemas en producción		

A.12.7.1	Controles de auditoría en sistemas de información.	SI	Los requisitos de auditoría y las actividades que incluyan verificación de sistemas de producción deben estar planeados y acordados para minimizar las disrupciones a los procesos de negocio.	
A.13	**SEGURIDAD EN COMUNICACIONES**			
A.13.1	Gestión de seguridad en redes	Asegurar la protección de la información en redes e instalaciones de procesamiento de datos		
A.13.1.1	Controles de red	SI	Las redes se deben gestionar y controlar para proteger la información en los sistemas y aplicaciones	
A.13.1.2	Seguridad de servicios de red	SI	Se deben identificar e incluir en los acuerdos de servicios de red aquellos mecanismos de seguridad, niveles de servicio y requisitos de gestión de servicios red.	
A.13.1.3	Segregación en redes	SI	Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en las redes	
A.13.2	Transferencia de información	Mantener la seguridad de la información transferida dentro de la organización y con cualquier entidad externa.		
A.13.2.1	Políticas y procedimientos para la transferencia de información	SI	Deben estar en su lugar políticas formales, procedimientos y controles para controlar la transferencia de información mediante el uso de los tipos de instalaciones de	

			comunicación.	
A.13.2.2	Acuerdos de transferencia de información	SI	Los acuerdos deben atender la transferencia segura de información del negocio entre la organización y partes externas.	
A.13.2.3	Mensajería electrónica	SI	La información involucrada en mensajería electrónica debe ser protegida de manera adecuada.	
A.13.2.4	Acuerdos de confidencialidad y no divulgación.	SI	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad y no divulgación de la información, que reflejan las necesidades de la organización respecto a la protección de la información.	
A.14	**ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**			
A.14.1	Requisitos de seguridad de los sistemas información	Asegurar que la seguridad de la información es parte de los sistemas de información a los largo de su ciclo de vida. También incluye los requisitos para los sistemas de información que proveen servicios en redes públicas.		
A.14.1.1	Análisis y especificación de requisitos en seguridad información	SI	Se deben incluir los requisitos relacionados con seguridad de la información en los requisitos de nuevos sistemas o las mejoras de los existentes.	
A.14.1.2	Aseguramiento de servicios de aplicaciones en redes públicas.	SI	Se debe proteger la información involucrada en servicios de aplicaciones que	

			transiten por las redes públicas, frente a actividad fraudulenta, disputa en contratos así como divulgación o autorización no autorizada.	
A.14.1.3	Protección de transacciones en servicios de aplicaciones,	SI	La información involucrada en transacciones en servicios de aplicaciones, debe estar protegida para prevenir la trasmisión incompleta, errores de enrutamiento, alteración o duplicación no autorizadas del mensaje o su reenvío.	
A.14.2	Seguridad en procesos de desarrollo y soporte	Asegurar que la seguridad de la información se diseña e implementa dentro del ciclo de desarrollo de los sistemas de información.		
A.14.2.1	Política de desarrollo seguro	SI	Se deben establecer reglas para el desarrollo de software y sistemas para los desarrollos de la organización	
A.14.2.2	Procedimiento de control de cambio en sistemas	SI	Se deben de controlar los cambios a los sistemas en el ciclo de vida de desarrollo mediante el uso de procedimientos formales de control de cambios.	
A.14.2.3	Revisión técnica de aplicaciones luego de cambios en plataformas de producción	SI	Cuando se realizan cambios en las plataformas de producción, las aplicaciones críticas para el negocio, deben ser revisadas y	

			probadas para asegurar que no hay impacto adverso en las operaciones o seguridad de la organización.	
A.14.2.4	Restricciones a cambios en los paquetes de software	SI	Se deben rechazar las modificaciones a los paquetes de software, limitándolas a los cambios necesarios. Todo cambio debe ser controlado estrictamente	
A.14.2.5	Principios de la ingeniería de sistemas seguros	SI	Se debe establecer, documentar, mantener y aplicar principios para la ingeniería de sistemas seguros en esfuerzos de implementación de sistemas de información	
A.14.2.6	Ambiente seguro de desarrollo	SI	Las organizaciones deben establecer y proteger adecuadamente los ambientes seguros de desarrollo para el desarrollo de sistemas y esfuerzos de integración que incluyan la totalidad del ciclo de vida de desarrollo.	
A.14.2.7	Desarrollo tercerizado	SI	La organización debe supervisar el desarrollo tercerizado de sistemas.	
A.14.2.8	Prueba de seguridad de los sistemas	SI	En el desarrollo se deben realizar pruebas de funcionalidad de la seguridad.	
A.14.2.9	Pruebas de aceptación de sistemas.	SI	Se deben establecer programas de pruebas de aceptación y sus	

			criterios para sistemas de información nuevos, actualizaciones y nuevas versiones.	
A.14.3	Datos de Prueba	Asegurar la protección de los datos durante las pruebas		
A.14.3.1	Protección de datos de pruebas	SI	Los datos de prueba deben seleccionarse con cuidado, protegidos y controlados.	
A.15	**RELACIONES CON LOS PROVEEDORES**			
A.15.1	Seguridad de la información en relaciones con los proveedores	Asegurar la protección de activos que sean accesibles por los proveedores.		
A.15.1.1	Política de seguridad de la información para relación con los proveedores	SI	Se deben acordar y documentar los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos.	
A.15.1.2	Incorporación de la seguridad en acuerdos con proveedores	SI	Debe establecerse y acordarse los requisitos relevantes en seguridad de la información con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proveer componentes para infraestructura de TI.	
A.15.1.3	Cadena de suministro para las tecnologías de la información y las comunicaciones.	SI	Los acuerdos con proveedores deben incluir requisitos para atender los riesgos de seguridad de la información asociados	

			con la información, los servicios de tecnologías de comunicación y la cadena de suministro de productos.	
A.15.2	Gestión de la entrada de servicios por parte del proveedor	Mantener un nivel acordado de seguridad de la información y de entrega de servicios en concordancia con los acuerdos con el proveedor.		
A.15.2.1	Supervisión y revisión de servicios por proveedores	SI	Se deben de gestionar los cambios en los servicios prestados por proveedores, incluyendo el mantenimiento y mejora de las políticas, procedimientos y controles de seguridad de la información, considerando la criticidad de la información del negocio.	
A.16	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**			
A.16.1	Gestión de incidentes y mejoras en seguridad de la información	Asegurar un enfoque consistente y eficaz para la gestión de incidentes de seguridad de la información.		
A.16.1.1	Responsabilidades y procedimientos	SI	Se deben establecer responsabilidades y procedimientos para asegurar una respuesta rápida, eficaz y ordenada a incidentes de seguridad de la información.	
A.16.1.2	Reportes de eventos de seguridad de la información	SI	Los eventos de seguridad de la información deben ser reportados a través de	

			los canales apropiados tan rápido como sea posible.	
A.16.1.3	Reporte de debilidades en la seguridad de la información	SI	Se debe exigir a los trabajadores y contratistas que usen los sistemas y servicios de información de la organización que tomen nota y reporten cualquier debilidad de seguridad de la información observada o sospechada en sistemas o servicios.	
A.16.1.4	Evaluación y decisiones en eventos de seguridad de la información	SI	Los eventos en seguridad de la información deben ser evaluados y decidir si son clasificados como incidentes de seguridad de la información.	
A.16.1.5	Respuesta a incidente se seguridad de la información	SI	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.	
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	SI	El conocimiento ganado del análisis y solución de incidentes de seguridad de la información debe ser usado para reducir la probabilidad e impacto de incidentes futuros.	
A.16.1.7	Recolección de evidencia	SI	La organización debe definir y aplicar procedimientos para identificar, reunir, adquirir y preservar información que pueda	

			servir como evidencia.	
A.17	**ASPECTOS DE SEGURIDAD EN LA GESTION DE CONTINUIDAD DEL NEGOCIO**			
A.17.1	Continuidad de la seguridad de la información	La seguridad de la información debe ser parte de la gestión de continuidad del negocio		
A.17.1.1	Planeación de la continuidad de la seguridad de la información	SI	La organización debe determinar sus requisitos de seguridad de la información y la continuidad de la gestión de seguridad de la información en condiciones adversas, por ejemplo una crisis o desastre.	
A.17.1.2	Implementar la continuidad de la seguridad de la información	SI	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad para la seguridad de la información durante una situación adversa.	
A.17.1.3	Verificar, revisar y evaluar la continuidad de la seguridad de la información	SI	La organización debe verificar a intervalos regulares los controles establecidos e implementados de continuidad de la seguridad de la información, para asegurar q ellos	

			permanecen válidos y son eficaces durante situaciones adversas.	
A.17.2	Redundancias	Asegurar la disponibilidad de las instalaciones de procesamiento de la información.		
A.17.2.1	Disponibilidad de las instalaciones procesamiento de información	SI	Las instalaciones de procesamiento de información deben ser implementadas con suficiente redundancia para cumplir los requisitos de disponibilidad.	
A.18	**CUMPLIMIENTO**			
A.18.1	Cumplimiento de los requisitos legales y contractuales	Evitar el incumplimiento de obligaciones legales, estatutarias, regulatorias o contractuales relacionadas con seguridad de la información y cualquier requisito de seguridad.		
A.18.1.1	Identificar requisitos legales y contractuales aplicables	SI	Todos los requisitos relevantes a nivel legislativo, estatutario, regulatorio y contractual así como el enfoque de la organización para cumplir con tales requisitos debe estar explícitamente identificado, documentado y actualizado para cada sistema de información y para la organización.	
A.18.1.2	Derechos de propiedad intelectual	SI	Se deben implementar procedimientos apropiados para	

			asegurar el cumplimiento de los requisitos legislativos, regulatorios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos propietarios de software.	
A.18.1.3	Protección de registros	SI	Los registros deben estar protegidos de su pérdida, destrucción, falsificación, acceso no autorizado y liberación o divulgación no autorizada de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio.	
A.18.1.4	Privacidad y protección de información identificable como personal	SI	Se debe asegurar la privacidad y la protección de información identificable como personal según se requiera en la legislación y regulación pertinente.	
A.18.1.5	Regulación de controles criptográficos	SI	Los controles criptográficos deben ser usados dando cumplimiento a los acuerdos relevantes así como a la legislación y regulaciones.	
A.18.2	Revisión de la seguridad de	Asegurar que la seguridad de la información se encuentra implementada y opera de acuerdo con las políticas y		

	la información	procedimientos de la organización		
A.18.2.1	Revisión independiente de la seguridad de la información	SI	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (ejemplo: objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) debe ser revisado de manera independiente a intervalos planeados o cuando ocurran cambios significativos.	
A.18.2.2	Cumplimiento con políticas de seguridad y estándares	SI	La dirección debe revisar regularmente el cumplimiento en el procesamiento de la información y sus procedimientos dentro de su área de responsabilidad, frente a las políticas de seguridad estándares y otros requisitos de seguridad.	
A.18.2.3	Revisión de cumplimiento técnico	SI	Los sistemas de información deben ser revisados regularmente en cuanto a su cumplimiento frente a las políticas de seguridad de la información de la organización y estándares.	

ANEXO B
MATRIZ DE ROLES Y RESPONSABILIDADES

Ver documento Excel adjunto.

CONTROL DE VERSIONES

ID	FECHA	DESCRIPCIÓN	ELABORADO	REVISADO	APROBADO
1	Año 2000	Creación del Manual SGC por Vp. de Informática	Olga Yamile Huertas	Francisco Pacheco	Mario Rosero
2	2005	Ajuste del Manual de Calidad de Informática ampliando el Alcance para uso Corporativo	Alba Claudia Zárate	Yanet García García	Mario Rosero
3	2006	Manual de Calidad de Informática Paso a ser de uso Corporativo absorbiendo las versiones manejadas en Informática	Alba Claudia Zárate	Norma Villanueva	Oscar Ortiz
4	2006	Manual de Calidad Corporativo ampliación para alcanza de Datos e Internet y Tesorería	Alba Claudia Zárate Erika López E.	Norma Villanueva	Oscar Ortiz
5	Oct/2007	Manual del Sistema de Gestión Empresarial – agrupando todos los sistemas de gestión	María Cecilia Quiasúa R.	Gustavo Adolfo Cala	Gustavo Adolfo Cala

6	Oct /2008	Mejoras Manual del Sistema de Gestión Empresarial Inclusión de Gestión de Riesgos y Aclaración que el Mapa de Procesos de ETB está en construcción y que se tiene como referencial e-TOM, se incluyó NTCGP:1000:2004	Maria Cecília Quiasúa/ Diana Carolina Mancera	Líderes de Procesos ETB Sol Mariana de La Rosa Flores Carlos Gustavo Alvarez	Fernando Panesso
7	Abr/2009	Mejoras Manual del Sistema de Gestión Empresarial. Inclusión de las observaciones realizadas por las áreas respecto a los temas tratados en el mismo y actualización de los objetivos corporativos. Se actualizó la versión de la Norma ISO 9001 de 2000 a 2008	Maria Cecília Quiasúa R / Carolina Restrepo Garrido	Sol Marina de La Rosa Flores, Dario Lara Caicedo, Adolfo Andrés Pérez V., Fernando Vergara Garcia Herreros Y Líderes de Procesos	Fernando Panesso
8	Nov/2009	Ajuste al Alcance del Sistema de Gestión e inclusión del control a procesos contratados externamente.	Maria Cecília Quiasúa R	Bureau Veritas	Fernando Vergara García Herreros

9	Oct./l 2010	Este documento Control de cambio y Revisiones Ejecutados al documento se saca deja como documento anexo al Manual que va antes de la Introducción, pues en sí no hace parte del Manual sino del control del mismo. Se ajusta la Tabla de contenido reordenando los temas contenidos en el manual. Se cambia la Introducción, la anterior estaba más enfocada en la historia de la Empresa que en el Sistema Integrado de Gestión. Se ajusta el Objetivo del Manual. Se ajusta el alcance. Se deja claro las exclusiones frente a los diferentes sistemas de gestión. El Numeral 2-Presentación de la Empresa se ajusta y actualiza, la Historia se deja como Anexo No.1, denominada como cronología. Se Incluye en el Capítulo 2 el Objeto Social de la Empresa y la Junta Directiva. En el Capítulo 2 se condensa el tema de Sistema de Control Interno y Ética en ETB.	Maria Cecília Quiasúa R	Líderes de Sistemas de Gestión	Fernando Vergara García Herreros

		Se reordena el tema de Cultura Corporativa y se incluyen los Valores Corporativos. Se reemplaza la anterior imagen de los atributos por la nueva imagen de Cultura en ETB Se eliminan las matrices relacionales de la misión, visión, objetivos y la política de Calidad. En su lugar se inserta el mapa estratégico corporativo con la nueva Misión, Visión y Objetivos estratégicos. Se incluye matriz, en donde se muestra el cambio y alcance al migrar de una política de Calidad a una Política Integral de Gestión.			Fernando Vergara García Herreros
9	Oct./l 2010	Se reordenan los capítulos de Diseño de Procesos en ETB y Sistema de Gestión Empresarial con el fin de que la secuencia sea lógica. Se Elimina la gráfica en la que se muestra la estructura y responsables del SGE De Igual manera se eliminó la gráfica de Organigrama Se Incluyó la Política Integral de Gestión. Se Incluyó un Anexo que corresponde a la Matriz Elementos Comunes en los	Maria Cecília Quiasúa R		

10	Sep./2012	El presente manual se redefine con base en la consolidación del Sistema Integrado de Gestión Corporativo - SIG generando cambios sobre el alcance del manual, normas y documentos de referencia, mapa de procesos, exclusiones, política del SIG, descripciones de los sistemas que lo componen, inclusión del modelo del Sistema Integrado de Gestión, estructura documental de la entidad, definición de los representantes por la dirección, inclusión del Anexo A correspondiente a Seguridad de la Información denominado Declaración de aplicabilidad (SOA).	Carolina Restrepo Garrido/ Lizeth Johanna Pinzón Pérez	Luis Armando López Bobadilla	Sergio González Guzmán Hernando Francisco Chica Zuccardi Mauricio Vasco Moscovith Javier Gutiérrez Afanador
11	Mar/2015	Se actualiza el Anexo A del Sistema de Gestión de Seguridad de la Información, bajo la nueva norma ISO/IEC 27001:2013 (14 dominios) Objetivos y Controles.	Clara Patricia Muñoz Jiménez	Luis Fernando Mancera	Comité Empresarial SGSI

12	Octubre/2016	Se actualiza el manual en su totalidad y es aprobado por el Comité Directivo SIG	Ana Paola Ramírez Luis Fernando Mancera	Natalia Gutiérrez	Comité Directivo SIG