DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN ORIENTADO AL ÁREA DE TECNOLOGÍA PARA COMBUSTIBLES LÍQUIDOS DE COLOMBIA S.A. ESP DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27001:2013

ALEJANDRO ÁLVAREZ ALONSO
RUBÉN DARÍO ESPITIA MANRIQUE

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, COLOMBIA
2016

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN ORIENTADO AL ÁREA DE TECNOLOGÍA PARA COMBUSTIBLES LÍQUIDOS DE COLOMBIA S.A. ESP DE ACUERDO CON EL ESTÁNDAR ISO/IEC 27001:2013

ALEJANDRO ÁLVAREZ ALONSO
RUBÉN DARÍO ESPITIA MANRIQUE

Trabajo de grado para optar al título de:
Especialista en Seguridad Informática

Asesor:
ING. LORENA OCAMPO CORREA

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, COLOMBIA
2016

Nota de aceptación:

_____

_____

_____

_____

_____

Firma decano de la facultad

_____

Firma primer jurado

_____

Firma segundo jurado

Bogotá, 28 de septiembre de 2016

DEDICATORIA

Dedicamos este trabajo a las futuras generaciones de especialistas en seguridad de la información, y a todos los profesores con los que tuvimos el honor de tener clase.

AGRADECIMIENTOS

Gracias a la Universidad Piloto por su constante enfoque en el compromiso y responsabilidad como profesionales frente a la seguridad y a nuestros familiares y amigos, que nos brindaron apoyo y confianza en nuestro trabajo.

CONTENIDO

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

pág.

LISTA DE CUADROS

pág.

LISTA DE ANEXOS

GLOSARIO

ACTIVO DE INFORMACIÓN: cualquier elemento físico, tecnológico o intangible que genera, almacena o procesa información y tiene valor para la organización, como bases de datos, archivos, programas, manuales, equipos de comunicaciones, la imagen de la empresa[1].

AMENAZAS: son aquellos factores externos que están fuera de nuestro control y que podrían perjudicar y / o limitar el desarrollo de la organización. Las amenazas son hechos ocurridos en el entorno que representan riesgos para la Entidad[2].

ANÁLISIS DE RIESGOS: método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado[3].

CONTROL: acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una compañía. Un control incluye entre otras: la definición de políticas, la puesta en marcha de procedimientos, la definición de guías, la definición de cambios en una estructura organizacional, o la ejecución de buenas prácticas que pueden ser de carácter administrativo, técnico o legal[4].

DECLARACIÓN DE APLICABILIDAD: documento que describe los objetivos de control y los controles pertinentes y aplicables para el sistema de gestión de seguridad de la información de la compañía[5].

---

[1] WORDPRESS. ¿Qué es un activo de información?. [En línea], [consultado el 25 de abril de 2016]. Disponible en: https://camiloangel.wordpress.com/2010/09/03/¿que-es-un-activo-de-informacion

[2] MINISTERIO DE TECNOLOGÍAS DE INFORMACIÓN. Glosario. [En línea], [consultado el 28 de septiembre de 2016]. Disponible en: www.mintic.gov.co/gestionti/615/articles-6099_recurso_2.docx › General

[3] WELIVE SECURITY. Análisis de riesgos. [En línea], [consultado el 25 de abril de 2016]. Disponible en: www.welivesecurity.com/la-es/2012/08/16/en-que-consiste-analisis-riesgos/

[4] INSTITUTO ESPAÑOL DE ANALISTAS. ¿Qué es control? [En línea], [consultado el 25 de abril de 2016]. Disponible en: ieaf.es/new/lideres-de.../control-y...riesgos.../1561-que-es-el-control-de-riesgos.html

[5] WELIVESECURITY. ¿Qué es declaración de aplicabilidad? [En línea], [consultado el 25 de abril de 2016]. Disponible en: www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa/

POLÍTICA DE SEGURIDAD: documento en el cual se estipulan las políticas con respecto a la seguridad de la información de la organización[6].

TRATAMIENTO DEL RIESGO: proceso de selección e implementación de medidas para modificar el riesgo[7].

[6] CARO Y CUERVO. ¿Qué es política de seguridad? [En línea], [consultado el 25 de abril de 2016]. [En línea], [consultado el 25 de abril de 2016]. Disponible en: Disponible en: www.caroycuervo.gov.co/ sites/.../POLÍTICA% 20DE%20 SEGURIDAD% 20ICC_0.pd

[7] ESCUELA DE ADMINISTRACIÓN, FINANZAS Y TECNOLOGÍA. ¿Qué son medidas de tratamiento? www.eafit.edu.co/.../Nota%20de% ase%2010%20Medidas%20de%20Tratamiento

RESUMEN

El presente trabajo define los requerimientos y controles que son requeridos para diseñar un sistema de gestión de seguridad de la información o SGSI de forma metódica y lógica, en una compañía como Combustibles Líquidos de Colombia, basado en objetivos claros de seguridad, y la identificación y tratamiento adecuado de los riesgos a los que está sometida la información.

Para lograr el diseño del SGSI y los Objetivos propuestos, el plan del proyecto se enmarca en el uso y referencia que proporciona la norma ISO/IEC 27001:2013, el cual permite promover un modelo con el cual se pueda establecer, diseñar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de Información.

Aunque está orientado al proceso de tecnología en Combustibles Líquidos de Colombia S.A. ESP, la metodología y los pasos definidos podrán ser aplicados en los demás procesos, hasta lograr un sistema Integrado con otros sistemas y la madurez del SGSI.

PALABRAS CLAVE: requerimientos, controles, proceso de tecnología, combustibles, seguridad,

INTRODUCCIÓN

En la actualidad, la gran mayoría de las compañías tienen procesos que son soportados, automatizados y gestionados por sistemas informáticos, en donde se busca que la información tenga las condiciones y atributos de confidencialidad, integridad y disponibilidad, para poder tomar decisiones y lograr el desarrollo de sus procesos con los menores riesgos posibles.

El diseño de un sistema de gestión de seguridad de la información o SGSI, se convierte en una necesidad para las organizaciones, no solo por la relación existente entre las personas, los procesos y la tecnología, sino por la necesidad de contar con políticas y pautas generales para una adecuada gestión de la seguridad de la información.

El SGSI permite orientar el negocio en la búsqueda de las condiciones y ambientes de seguridad requeridas para el desarrollo de sus procesos, mediante la identificación de posibles riesgos, amenazas y vulnerabilidades, que puedan afectar los atributos de la seguridad de la información y la continuidad de los procesos.

El desarrollo de este trabajo es una propuesta de cómo abordar el desarrollo de un sistema de gestión de seguridad para brindar la confianza necesaria a la empresa, a los socios de negocio y a los usuarios.

1. PROBLEMA

1.1 DEFINICIÓN DEL PROBLEMA

Muchas organizaciones cuentan con mecanismos y controles de seguridad, que reducen los efectos de estar expuestos a constantes amenazas y problemas derivados de fallas de seguridad; tanto en aplicaciones como en infraestructura tecnológica; sin embargo, todos los días se desarrollan e implementan nuevas técnicas y estrategias que aprovechan vulnerabilidades que antes no se habían identificado, con el mismo propósito de lograr efectos negativos en la operación y los objetivos del negocio, llegando en algunos casos a tener acceso al recurso más valioso para una organización, la información.

El diseño de un sistema de seguridad de la información es solo el inicio del desarrollo de los esquemas, estrategias y modelos, que la organización debe adoptar para lograr una adecuada gestión de la seguridad, y no solo obedece a una buena práctica; sino a una necesidad de todas las organizaciones, pues proporciona a la alta gerencia información suficiente para la toma de decisiones y reduce el impacto de dichos efectos negativos.

En el marco de este contexto, se propone el desarrollo e implementación de un sistema de gestión de seguridad de información – SGSI en Combustibles Líquidos de Colombia S.A. ESP, el cual permitirá identificar y tratar posibles riesgos asociados a la seguridad de la información.

1.2 PLANTEAMIENTO DEL PROBLEMA

¿De qué manera se puede proteger los activos de información del proceso de tecnología en una empresa como Combustibles Líquidos de Colombia S.A. ESP?

1.3 JUSTIFICACIÓN

La mayor parte de la información de Combustibles Líquidos de Colombia S.A. ESP reside en equipos informáticos, medios de almacenamiento y servidores de aplicaciones, lo que comúnmente se conoce como sistemas de información. Estos sistemas de información aunque son solo para el uso interno de los procesos y de las personas que tienen acceso, están sujetos a riesgos y amenazas que pueden generarse por múltiples factores internos y externos, razón por la cual se deben identificar los posibles riesgos físicos que puedan afectar su disponibilidad.

Hoy en día Combustibles Líquidos de Colombia S.A. ESP no cuenta con una metodología que le permita identificar riesgos y amenazas relacionados con la información y el uso de la tecnología, que la protejan de posibles robos de identidad, virus, robos de información y/o espionaje industrial, por nombrar algunos riesgos que pueden impactar la confianza de los clientes de Combustibles Líquidos de Colombia S.A. ESP y la imagen de la compañía en el mercado.
Para proteger a la organización de posibles riesgos y amenazas, es necesario diseñar un sistema de gestión de seguridad de la información, bajo una metodología que permita establecer los procedimientos con los cuales se garantice la seguridad de la información.

1.4 OBJETIVOS

1.4.1 Objetivo general. Diseñar un sistema de gestión de seguridad de información - SGSI, que permita identificar y tratar los riesgos a los cuales se ve expuesto Combustibles Líquidos de Colombia S.A. ESP en el área de tecnología de acuerdo con el estándar ISO/IEC 27001:2013.

1.4.2 Objetivos específicos

- Valorar los activos de información asociados al proceso de tecnología, describiendo el estado actual de cada uno de ellos, haciendo uso del estándar ISO/IEC 27001:2013.

- Identificar y analizar los riesgos a los que están expuestos los activos de información del área de tecnología para Combustibles Líquidos de Colombia S.A. ESP.

- Proponer el tratamiento de los riesgos identificados.

- Proponer la política de seguridad de la información para Combustibles Líquidos de Colombia S.A. ESP.

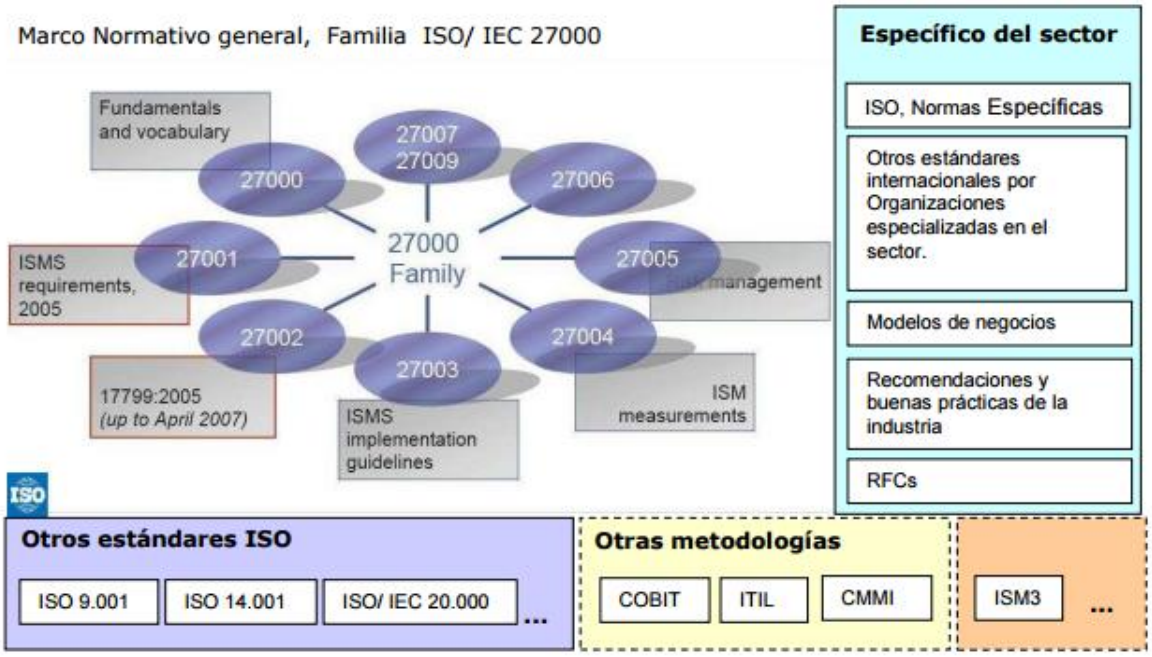
2. MARCO DE REFERENCIA

2.1 MARCO TEÓRICO

Dentro de los modelos y normas que pueden ser utilizados para la implementación de un sistema de gestión de la seguridad de la información se encuentra enmarcada la norma ISO/IEC 27001:2013, aprobada y publicada por la ISO - International Organización for standardization. Esta norma proporciona recomendaciones a partir de las mejores prácticas en la gestión de la seguridad de la información, dirigida a todos los responsables de iniciar, implantar o mantener sistemas de gestión de la seguridad (SGSI), partiendo de los conceptos de confidencialidad, integridad y disponibilidad de la información.

La ISO/IEC 27001:2013 hace parte de la familia de normas de la serie ISO/IEC 27000, las cuales contienen mejores prácticas para desarrollar, implementar y mantener especificaciones para los sistemas de gestión de la seguridad de la información (SGSI). La figura 1 muestra la relación que tiene cada una de las normas que componen la familia 27000:

Figura 1. Familia ISO/IEC 27000



Fuente: BRYDEN, Alan, COPANT Seminar on Security Standards, La Paz, 25 de abril de 2006. [En línea], [consultado el 25 de abril de 2016]. Disponible en: http://www.iso.org/iso/livelinkgetfile?llNodeId=21657&llVolId=-2000

La 27001 es la norma más importante de la familia, dado que especifica los requisitos para la implantación del SGSI. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Tiene relación con cada norma de la familia de la siguiente forma:

- ISO/IEC 27000, es un vocabulario estándar para el SGSI.

- ISO/IEC 27002, Information technology - Security techniques - Code of practice for information security management. Es código de buenas prácticas para la gestión de seguridad de la información.

- ISO/IEC 27003, son directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001.

- ISO/IEC 27004, son métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información.

- ISO/IEC 27005, trata la gestión de riesgos en seguridad de la información. Es la que proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001.

- ISO/IEC 27799:2008 - Es una guía para implementar ISO/IEC 27002 en la industria de la salud.

- ISO/IEC 27035:2011 - Seguridad de la información – Técnicas de Seguridad – Gestión de Incidentes de Seguridad. Este standard hace foco en las actividades de: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades.[8]

La norma 27002, se considera de gran importancia, pues es el código de buenas prácticas para un Sistema de gestión de la seguridad de la información (SGSI); está organizada en 14 dominios, 35 objetivos de control y 114 controles apuntados a las categorías principales dentro de un sistema de gestión de seguridad de la información. Los dominios sobre los que se establece la seguridad, se pueden esquematizar cómo se muestran en la figura 2, partiendo de la Organización como aspecto estratégico, hasta los procedimientos de un SGSI, consideraos como su parte operativa:

[8]BLOG DE BITCOMPANY. Los beneficios que ofrece el Project Management, COBIT y normas ISO a las organizaciones que lo implementan. [En línea], [consultado el 25 de abril de 2016]. Disponible en: www.bitcompany.biz/.

Figura 2. Dominios de ISO/IEC 27001:2013

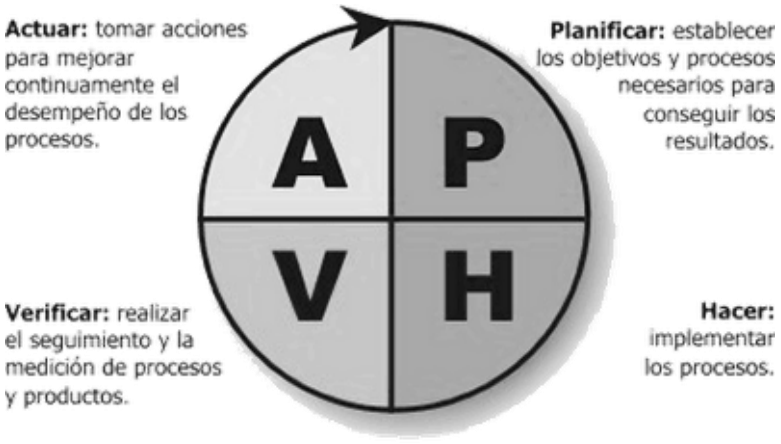
Fuente: Instituto Uruguayo de Normas Técnicas. Normalización: ISO 27000. **[En línea], [consultado el 25 de abril de 2016]. Disponible en: http://www.unit.org.uy/vista/html/_ Ing./normalización/ sist_27000_ que.png**

En la figura 2 se identifican los dominios que cambiaron frente a la versión del 2005 de la norma, los que se marcan con línea punteada roja.

Algunas organizaciones han venido alineando y adecuando previamente de forma rigurosa sus diferentes sistemas de información y sus procesos de trabajo a las exigencias de las normativas legales, tal y como la Ley 1581 de 2012 Habeas Data y el decreto 1377 de 2013, la circular 022 de 2012 de la Superintendencia Financiera de Colombia, las directrices establecidas por la presidencia de la república para el gobierno en línea, lo cual ha permitido de alguna u otra forma, que se hayan acercado a la seguridad de la información.

Al tratarse de un sistema de gestión, el mismo, debe hacer uso de una de las principales herramientas de mejoramiento continuo en las organizaciones, el ciclo conocido como “Ciclo de Deming o PDA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar), en donde cada etapa del ciclo permite direccionar al sistema de gestión. Es una herramienta utilizada ampliamente por los sistemas de gestión de la calidad (SGC) con el propósito de permitirle a las empresas una mejora integral. En la figura 3, se puede ver el ciclo en la 27001:

Figura 3. Ciclo PHVA en ISO/IEC 27001

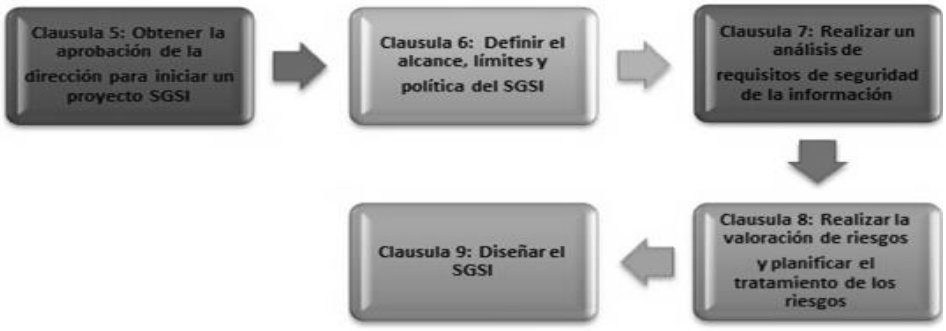


Fuente: Juran, J. (2012). Total igualdad de producto por igualdad de proceso. [En línea], [consultado el 25 de abril de 2016]. Disponible en: http://www.totalqualidade.com.br/2012/09/

En la etapa de **PLANIFICAR,** se definen los objetivos y cómo lograrlos, esto de acuerdo a políticas organizacionales y necesidades de los clientes; En la etapa de **HACER,** se ejecuta lo planeado; En la etapa de **VERIFICAR,** se comprueba que se hayan ejecutado los objetivos previstos mediante el seguimiento y medición de los procesos; Y en la última etapa de **ACTUAR,** se realizan las acciones para el mejoramiento del desempeño de los procesos, se corrigen las desviaciones, se estandarizan los cambios, se realiza la formación y capacitación requerida y se define como monitorearlo.

La ISO 27003 explica el proceso de implementación, para lo cual propone desarrollar la implementación por medio de las siguientes 5 fases, Ver figura 4:

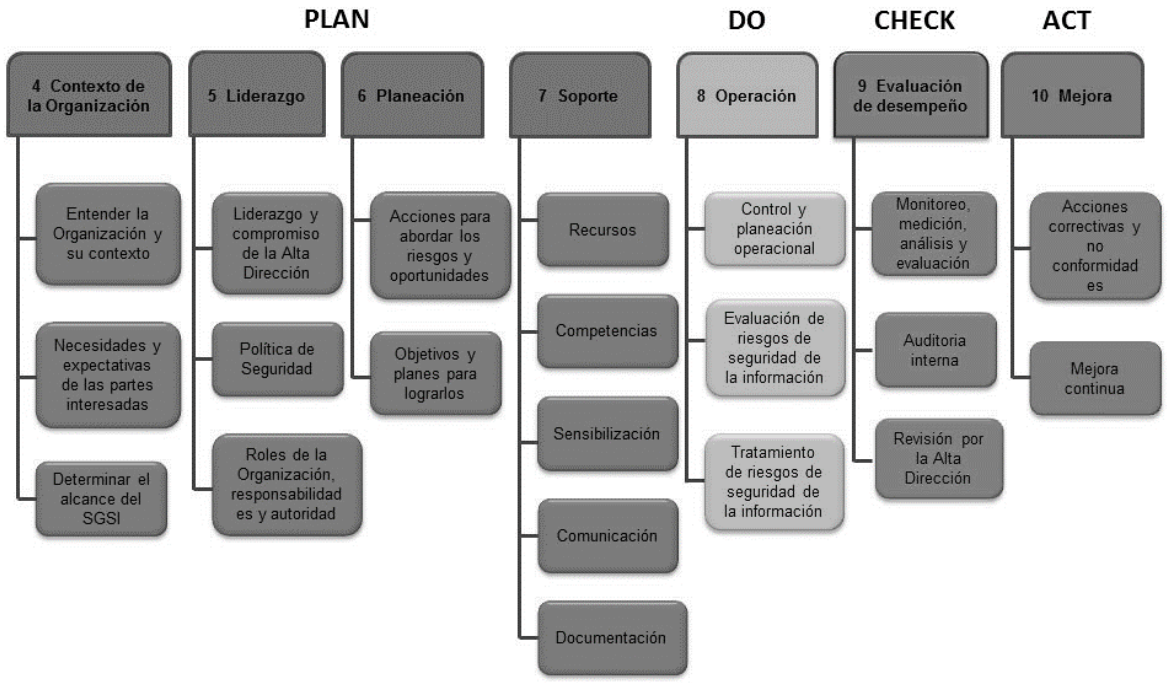
Figura 4. Proceso de implementación según ISO 27003



Fuente: MORENO, Fernando. ISO 27003 (SGSI) Ayuda y guía para implementar un SGSI. CISM 2015. [En línea], [consultado el 25 de abril de 2016]. Disponible en: https://es.scribd.com/doc/.../**ISO**-**27003**-**SGSI**-**Ayuda**-**y**-**Guia**-**Para**-**Implementar**-en-

De esta forma, cada etapa del ciclo, tiene actividades que permiten desarrollar el SGSI de forma ordenada y sistemática, tal y como se muestra en la figura 5, en la cual se detalla cada etapa:

Figura 5. Ciclo PDCA en 27001 detallado



Fuente: WORDPRESS. Ciclo pdca en 27001-2013. [En línea], [consultado el 25 de abril de 2016]. Disponible en: https://trabajoscun.files.wordpress.com/2014/ 03/ciclo-pdca-en-27001-2013

En la figura 5, cada etapa del ciclo de Deming, relaciona las diferentes actividades o controles que se deben desarrollar en la norma, de modo que se pueda hacer un enfoque sobre el sistema de gestión de seguridad de la información, como el concepto central sobre el que se construye la norma NTC-ISO/IEC 27002:2013.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. La gestión de la seguridad de la información fomenta la importancia de:

- Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información.

- Implementar y operar controles para manejar los riesgos de la seguridad de la información.

- Monitorear y revisar el desempeño del SGSI.

- Realizar mejoramiento continuo en base a la medición del objetivo.

La norma ISO 27001 se convierte en la guía a seguir a través de sus diferentes dominios, lo que permite, implementar, operar, monitorear, revisar y realizar la mejora continua del sistema de gestión de seguridad de información – SGSI, a su vez permite entender e interiorizar en Combustibles Líquidos de Colombia S.A. ESP el concepto de la seguridad de la información.

En Colombia, el instituto Colombiano de normas técnicas - ICONTEC adopta la norma ISO/IEC 27001:2013 por traducción bajo la referencia ISO/IEC 27001. En el cuadro 1 se relacionan los requisitos que se consideran indispensables para que el funcionamiento de un SGSI:

Cuadro 1. Requisitos de la norma ISO/IEC 27001:2013.

Numeral norma ISO-IEC 27001:2013	**Descripción general**
4. Contexto de la organización	La organización debe estar consciente de las cuestiones internas y externas que podrían influir en los resultados deseados de la seguridad de la información, así como determinar su alcance, límites y capacidad, garantizando que el SGSI cumpla los requerimientos de la norma.
5. Liderazgo	La alta gerencia de la organización debe liderar el proceso del SGSI verificando que se cumplan los requerimientos de la norma, garantizando los recursos, documentando las políticas y objetivos de seguridad propuestos, asignando las responsabilidades para cada una de las actividades y promoviendo el mejoramiento continuo.
6. Planificación	La organización debe escoger una metodología de clasificación, análisis y evaluación de riesgos, formando criterios para establecer los controles de seguridad y así mantener los niveles de riesgo a un nivel aceptable de acuerdo a las políticas y objetivos de seguridad.
7. Soporte	La organización debe velar por comunicar las políticas de seguridad de la información a sus empleados y que éstos se comprometan al mejoramiento continuo del SGSI. A su vez, también se deben garantizar los recursos y la cualificación de las personas para llevar a cabo cada actividad. También se deben generar los documentos que exige la norma y que éstos tengan su nivel de clasificación.
8. Operación	La organización debe documentar y planear los procesos para llevar a cabo las actividades, incluyendo las valoraciones de riesgos de la seguridad de la información y el plan de tratamiento de riesgos.
9. Evaluación del desempeño	La organización debe velar el desempeño de la seguridad de la información y medir la eficacia del SGSI, mediante auditorías internas a intervalos planificados, con el fin de verificar si se están cumpliendo con los objetivos y políticas de seguridad así como con la norma.
10. Mejora	La organización debe aplicar las acciones correctivas y promover un mejoramiento continuo.
Fuente: ISO/IEC 27001. ISO 27001 - Sistema de gestión de la seguridad de la información: requisitos. [En línea], [consultado el 25 de abril de 2016]. Disponible en: www.gesconsultor.com/iso-27001.html	

El establecimiento del SGSI se fundamenta en los siguientes documentos y registros requeridos por la revisión 2013 de la norma ISO/IEC 27001, descritos en los cuadros 2 y 3.

Cuadro 2. Documentación Requerida por la norma ISO/IEC 27001:2013.

Documentos	Cláusula ISO 27001:2013
El alcance del sistema de gestión de seguridad de la información	4.3
Política de seguridad de la información y objetivos	5.2 y 6.2
Metodología de evaluación y tratamiento de riesgos	6.1.2
Declaración de aplicabilidad	6.1.3 d
Plan de tratamiento de riesgo	6.1.3 e y 6.2
Informe sobre evaluación de riesgos	8.2
Definición de roles y responsabilidades de seguridad	A.7.1.2 y A.13.2.4
Inventario de activos	A.8.1.1
Uso aceptable de los activos	A.8.1.3
Política de control de acceso	A.9.1.1
Procedimientos de operación para gestión de TI	A.12.1.1
Principios de ingeniería de sistemas seguros	A.14.2.5
Política de seguridad para proveedores	A.15.1.1
Procedimiento para gestión de incidentes	A.16.1.5
Procedimientos de Continuidad de negocio	A.17.1.2
Requerimientos legales, regulatorios y contractuales	A.18.1.1
Fuente: ISO/IEC 27001. ISO 27001 - Sistema de gestión de la seguridad de la información: requisitos. [En línea], [consultado el 25 de abril de 2016]. Disponible en: www.gesconsultor.com/iso-27001.html	

De igual forma los siguientes registros son esenciales:

Cuadro 3. Registros mínimos obligatorios por la norma ISO/IEC 27001:2013.

Registros Obligatorios	Cláusula ISO 27001:2013
Registros de formación, habilidades, experiencia y calificaciones	(cláusula 7.2)
Seguimiento y resultados de medición	(cláusula 9.1)
Programa de auditoría interna	(cláusula 9.2)
Resultados de auditorías internas	(cláusula 9.2)
Resultados de la Revisión por Dirección	(cláusula 9.3)
Resultados de acciones correctivas	(cláusula 10.1)
Registros de las actividades de usuario, excepciones y eventos de seguridad	(cláusulas A.12.4.1 y A.12.4.3)
Fuente: ISO/IEC 27001. ISO 27001 - Sistema de gestión de la seguridad de la información: requisitos. [En línea], [consultado el 25 de abril de 2016]. Disponible en: www.gesconsultor.com/iso-27001.html	

2.1.1 Conceptos clave

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de Riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Estimación de Riesgos: Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables.

Evaluación de Riesgos: Proceso global de identificación, análisis y estimación de riesgos.

Impacto: El costo para la empresa de un incidente (de la escala que sea), que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperada o no deseado que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

2.2 MARCO NORMATIVO

En el cuadro 4 se describe la regulación aplicable y relacionada al proceso establecimiento de un SGSI en Combustibles Líquidos de Colombia S.A. ESP:

Cuadro 4. Regulación aplicable

Regulación Aplicable	Descripción
Ley 1266 del 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 1581 del 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 1377 del 2012	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley 1273 del 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.
Norma ISO 27001 del 2013	Establecer requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un Sistema de gestión de la seguridad de la información.
Decreto 2952 del 2010	Reglamenta los artículos 12 y 13 de la Ley 1266 de 2008, mediante la cual se dictaron 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.
Fuente: Autores	

3. SITUACIÓN ACTUAL

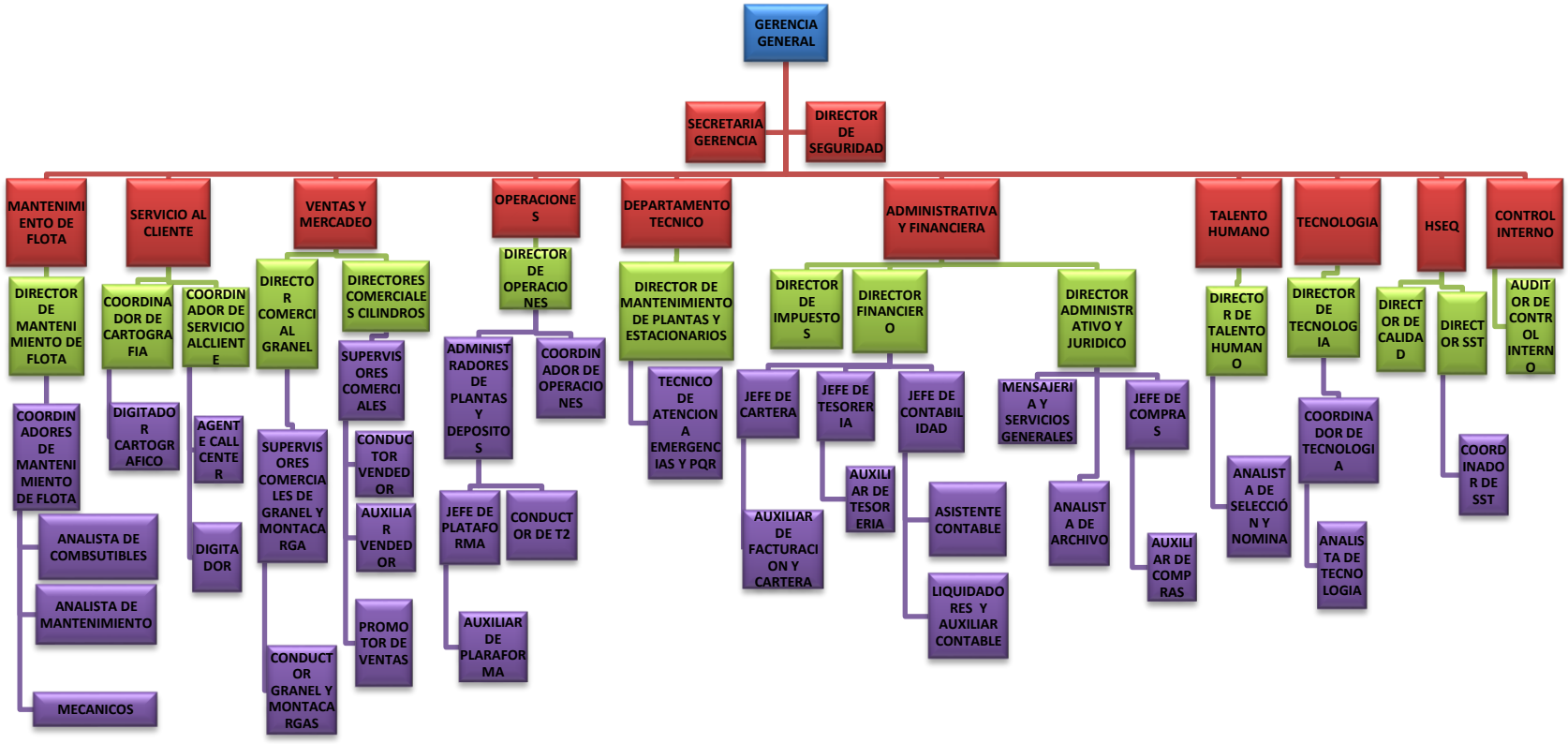
Combustibles Líquidos de Colombia S.A. ESP es una empresa de servicios públicos domiciliarios, que distribuye y comercializa gas licuado de petróleo (GLP). Hace apertura y abastece los puntos de venta, siendo este su principal factor diferenciador. Suministra GLP en cilindros directamente a usuario final y en tanques estacionarios, garantizando siempre la disponibilidad del producto. Su misión es la de ofrecer el mejor servicio de GLP en forma eficiente, confiable y continua, al alcance de todos sus usuarios y adaptable a sus necesidades.

La Misión: Se define en ofrecer el mejor servicio de GLP en forma eficiente, confiable y continua, al alcance de todos sus usuarios y adaptable a sus necesidades.

La Visión: Se define en ser una compañía agradable para trabajar, rentable y preferida por los consumidores de GLP.

Organigrama: La estructura organizacional de Combustibles Líquidos de Colombia S.A. ESP, se compone de estructuras departamentales. El área de tecnología está compuesta por el director de tecnología y el coordinador de tecnología. (Ver figura 6)

Figura 6. Organigrama de Combustibles Líquidos de Colombia S.A. E.S.P

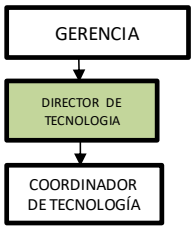


Fuente: Combustibles Líquidos de Colombia S.A. ESP

Las funciones del director de tecnología son las siguientes (Ver Figura 7):

Figura 7. Objetivo del cargo de director de tecnología de Combustibles Líquidos de Colombia S.A. E.S.P.

IDENTIFICACION DEL CARGO	
Cargo: DIRECTOR DE TECNOLOGÍA	
Cargo Superior Inmediato: GERENTE GENERAL	**Area del Cargo: TECNOLOGÍA**
Unidad Matriz: TECNOLOGÍA	**Numero de personas a Cargo: 0**

OBJETIVO DEL CARGO	ESTRUCTURA ORGANIZACIONAL
Planear, organizar, dirigir y controlar las estrategias necesarias para la implementación y mejoramiento de los sistemas de Información y comunicaciones de datos, voz e imágenes de la empresa, así como de la infraestructura tecnológica para su manejo eficiente.	

COMBUSTIBLES LÍQUIDOS DE COLOMBIA S.A. ESP. Sistema de Gestión de Calidad. [En línea], [consultado el 25 de abril de 2016]. Disponible en: **Combustibles-LÍQUIDOS-de-Colombia.**

- Dirigir los procesos de instalación, mantenimiento y operación de los equipos de red de CLC, INVERCOLSA y PROGASUR.

- Dirigir los cambios en las aplicaciones corporativas.

- Llevar control constante de los inventarios de activos tecnológicos.

- Velar por el cumplimiento del cronograma de mantenimiento a equipos tecnológicos.

- Velar por que la red de la compañía sea segura e inviolable, manteniendo la estructura de la red actualizada.

- Dirigir los proyectos tecnológicos planteados.

- Dirigir todos los procesos de implementación de CLC.

- Definir y poner en práctica las estrategias necesarias para la implantación y mejoramiento de los sistemas de información y comunicaciones de datos, voz e imágenes de la empresa, así como de la infraestructura tecnológica para su manejo eficiente.

- Realizar mejora continua al área mediante la aplicación y actualización de políticas en procesos y procedimientos del área alineados bajo el sistema de gestión de la calidad.

- Llevar control de las compras tramitadas por el área de tecnología.

- Dirigir los procesos de contratación del área de tecnología.

- Firmar los Paz y Salvo de los empleados que se retiran de la empresa.

Las funciones del coordinador de tecnología son (Ver figura 8):

Figura 8. Objetivo del cargo de coordinador de tecnología de Combustibles Líquidos de Colombia S.A. E.S.P

<table>
<tr><th colspan="3">IDENTIFICACION DEL CARGO</th></tr>
<tr><td colspan="3">Cargo: COORDINADOR DE TECNOLOGÍA</td></tr>
<tr><td colspan="2">Cargo Superior Inmediato: GERENTE GENERAL</td><td>Area del Cargo: TECNOLOGÍA</td></tr>
<tr><td colspan="2">Unidad Matriz: TECNOLOGÍA</td><td>Numero de personas a Cargo: 0</td></tr>
<tr><th colspan="2">OBJETIVO DEL CARGO</th><th>ESTRUCTURA ORGANIZACIONAL</th></tr>
<tr><td colspan="2">Desarrollar, modificar o implementar sistemas para el procesamiento electrónico de información según los requerimientos de los clientes internos.</td><td>GERENCIA
↓
DIRECTOR DE TECNOLOGIA
↓
COORDINADOR DE TECNOLOGÍA</td></tr>
</table>

Fuente: COMBUSTIBLES LÍQUIDOS DE COLOMBIA S.A. ESP. Sistema de Gestión de Calidad. [En línea], [consultado el 25 de abril de 2016]. Disponible en: Combustibles-líquidos-de-Colombia.

Las funciones del auxiliar de tecnología son:

- Administrar y coordinar los procesos de instalación, mantenimiento y operación de los equipos que manejan las redes internas y externas de las compañías CLC, Invercolsa, Progasur y Alcanos: (Servicio de Red: Internet, seguridad de borde sonicwall, red de datos, backup, seguridad de información, seguridad de cámaras, control de acceso al sistema, asterisk, comunicaciones móviles, redes eléctricas e infraestructura.

- Consultar con los clientes internos (CLC, Invercolsa, Progasur, Alcanos y Confedegas) sus requerimientos y da solución mediante la Mesa de Ayuda.

- Administrar el servicio de correo de Google Apps de CLC - Invercolsa y Progasur.

- Administrar el licenciamiento de equipos y servidores (Windows, Antivirus).

- Controlar los inventarios tecnológicos de CLC e Invercolsa a nivel nacional, mediante el CRM (Salesforce) y Drive.

- Realizar visitas de mantenimiento, asesoría y servicio técnico al personal de CLC e Invercolsa con el fin de asegurar el funcionamiento de los productos respondiendo a cada solicitud en el menor tiempo posible.

- Velar por que la red de la compañía sea segura e inviolable, manteniendo la estructura de la red actualizada.

- "Coordinar, realizar y hacer seguimiento de las actividades relacionadas con el diseño, montaje,

- instalación, pruebas, contratación y control de los proyectos tecnológicos que desarrolla la compañía."

- Coordinar y ejecutar la implementación de la normatividad técnica sobre esquemas de infraestructura tecnológica (ISO 27001/2013 e ITIL).

- Definir y poner en práctica las estrategias necesarias para la implantación y mejoramiento de los sistemas de información y comunicaciones de datos, voz e imágenes de la empresa, así como de la infraestructura tecnológica para su manejo eficiente.

- Realizar mejora continua al área mediante la aplicación y actualización de políticas en procesos y procedimientos del área alineados bajo el sistema de gestión de la calidad.

- Realizar el alistamiento de equipos tecnológicos para el personal que ingresa a la compañía y realizar la entrega formal (acta de entrega) registrándolo en el CRM-Salesforce para garantizar el control de inventarios.

- Recibir los equipos y verificar su estado en el momento que se retira una persona de la compañía para garantizar el control de inventarios; así como autorizar y firmar la paz y salvo sobre estos equipos para la persona que se retira.

- Firmar los paz y salvo de los empleados que se retiran de la empresa.

Las funciones del auxiliar de tecnología son (Ver figura 9):

Figura 9. Objetivo del cargo de auxiliar de tecnología de Combustibles Líquidos de Colombia S.A. E.S.P.

IDENTIFICACION DEL CARGO	
Cargo: Auxiliar de tecnologia	
Cargo superior inmediato: Coordinador de tecnologia	**Area del cargo: TECNOLOGIA**
Unidad Matriz: TECNOLOGIA	**Numero de personar a cargo: 0**

OBJETIVO DEL CARGO	ESTRUCTURA ORGANIZACIONAL
Soportar a los usuarios internos de la compañía en cuanto a tecnologia trata	GERENCIA DIRECTOR TECNOLOGIA COORDINADOR TECNOLOGIA AUXILIAR TECNOLOGIA

Fuente: COMBUSTIBLES LÍQUIDOS DE COLOMBIA S.A. ESP. Sistema de Gestión de Calidad. [En línea], [consultado el 25 de abril de 2016]. Disponible en: Combustibles**-LÍQUIDOS-de-Colombia.**

- Brindar soporte a los usuarios internos de CLC en cuento a requerimientos de tecnología trata.

- Tramitar los formatos definidos en el sistema de gestión de calidad, tales como actas de entrega, de devolución política de uso de recursos tecnológicos, formato de inventarios

- Realizar visitas periódicas a las plantas y depósitos según cronograma tramitando mantenimientos a equipos tecnológicos.

- Realizar mantenimiento a equipos tecnológicos en general.

- Velar por el eficiente funcionamiento de los equipos tecnológicos.

- Prestar un servicio excepcional a los usuarios cada que se reporte un requerimiento en la plataforma de Help Desk.

- Dar soporte en los tiempos establecidos como meta en el sistema de gestión de calidad.

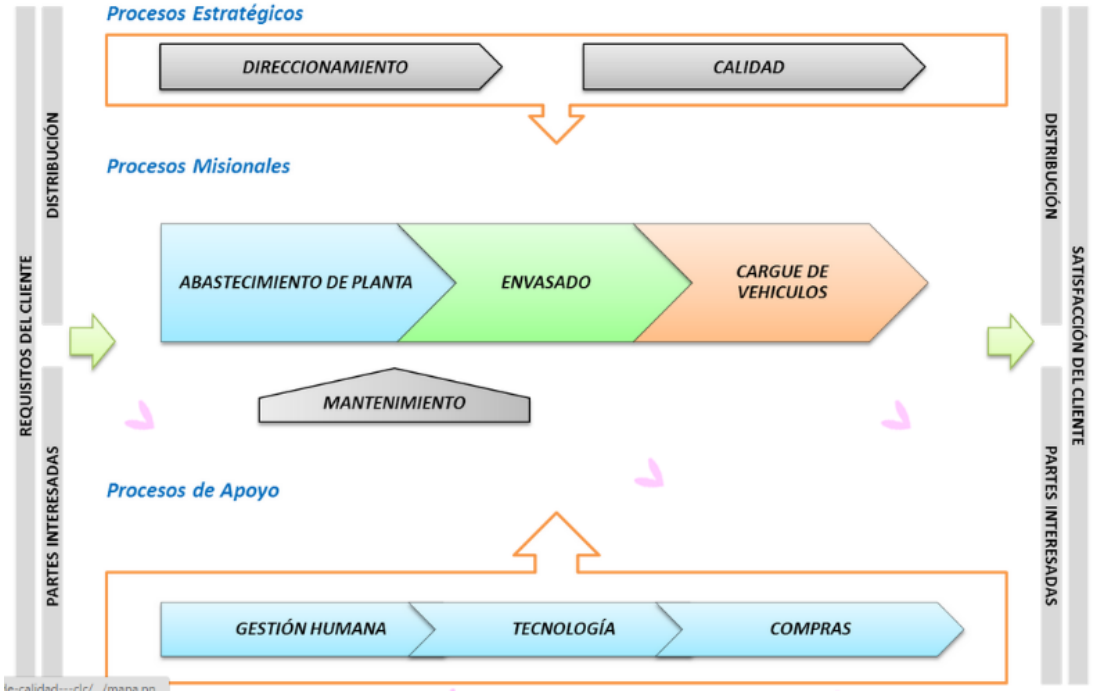
3.1 MAPA DE PROCESOS

Combustibles Líquidos de Colombia S.A. ESP cuenta con un sistema de gestión de calidad conocido comúnmente como el SGC, el cual se encuentra avalado y certificado bajo la ISO 9001:2008 por ICONTEC con fecha de aprobación 2015/04/15 y de vencimiento 2018/04/14, el cual tiene como alcance, la operación de envasado de gas licuado de petróleo (GLP) en cilindros de marca y cisternas.

Dicho sistema de gestión ya implementado en Combustibles Líquidos de Colombia S.A. ESP contiene su respectiva política y objetivos documentados en sus respectivos sistemas de información en los que no se profundiza mucho en este proyecto, aunque como lo menciona el marco teórico surge una alineación entre ambos sistemas.

Los procesos que ponen en funcionamiento la actividad económica de Combustibles Líquidos de Colombia S.A. ESP, permiten visualizar la posición y/o función que cumple dentro del mismo, el proceso de tecnología. (Ver figura 10)

Figura 10. Mapa de procesos de Combustibles Líquidos de Colombia SA ESP



Fuente: COMBUSTIBLES LÍQUIDOS DE COLOMBIA S.A. ESP. Sistema de Gestión de Calidad. [En línea], [consultado el 25 de abril de 2016]. Disponible en: Combustibles-**LÍQUIDOS-de-Colombia.**

El proceso de tecnología, es un proceso de apoyo, el cual tiene como objetivo prestar el servicio de administración y soporte de la infraestructura tecnológica y sus plataformas, para asegurar el funcionamiento operativo de la compañía. El alcance de este proceso es: Todos los procesos. El responsable del proceso es: El director de tecnología, con su respectivo suplente, el coordinador de tecnología

Las entradas del proceso son:

- Lineamientos gerenciales.
- Requerimientos de mesa de ayuda.
- Requerimientos de proveedores.

Las salidas del proceso son:

- Cierre de las solicitudes de servicios (Helpdesk).
- Aplicación de las configuraciones.
- Entrega de activos fijos.
- Ejecución del programa de mantenimiento.
- Registros.

Recursos del proceso:

- Recursos Tecnológicos:
    - Equipos: Computadores, Telefónicos.
    - Software: Salesforce, Qlikview, CGUNO, Saasmaint, Arcgis.
- Recursos Locativos: Infraestructura.
- Recurso Humano.

Indicadores del proceso:

- Nivel de Atención Casos Helpdesk, con una meta de 36 horas y frecuencias mensual.
- Satisfacción cliente interno, con una meta cualitativa de: “satisfecho” y frecuencia mensual.

Requisitos del Proceso en su desarrollo:

- Control de Documentos
- Control de Registros
- Infraestructura.
- Seguimiento y Medición de los Procesos.
- Mejora

En cuanto a las políticas implementadas y en funcionamiento en el proceso de tecnología, se cuenta con la política de uso de recurso tecnológico, la cual se

encuentra codificada en el sistema de gestión de calidad con el código R5-O001, la cual describe su objetivo en “Definir las políticas, disposiciones y procedimientos para la administración, el uso adecuado y seguro de los recursos tecnológicos y de servicio de Combustibles Líquidos de Colombia S.A. E.S.P. y garantizar la operación de la compañía.”; limita su alcance a todos los sistemas, versiones y plataformas instaladas en Combustibles Líquidos de Colombia S.A.. E.S.P. debe ser conocido e implementado por todos los usuarios de la compañía. Describe las buenas prácticas que deben seguir los usuarios de Combustibles Líquidos de Colombia S.A. ESP para utilizar de manera eficiente los recursos tecnológicos, orientando la misma a procedimientos de obligatorio cumplimiento para la conservación y cuidado de los ya mencionados recursos tecnológicos.

Dentro del proceso de tecnología se encuentran implementados los siguientes procedimientos formales codificados por el sistema de gestión de calidad, descritos por los siguientes códigos y títulos:

- R5-I001 Instructivo respaldo de información de estaciones de trabajo (Ver anexo I): Este documento realiza una descripción paso a paso de la respectiva configuración en los equipos de cómputo para llevar a cabo un Back Up a través de la herramienta gratuita SyncToy.

- R5-I002 Registro de casos mesa de ayuda (Ver anexo E): Este documento describe el procedimiento que deben seguir los usuarios para hacer el registro de un caso al área de tecnología para realizar el respectivo seguimiento y soporte al requerimiento escalado.

- R5-I003 Seguimiento de software instalado (Ver anexo G): Este documento describe el procedimiento que debe seguir el área de tecnología para realizar el seguimiento estricto al software instalado en los equipos tecnológicos propiedad de Combustibles Líquidos de Colombia S.A. ESP

- R5-P001 Procedimiento gestión de recursos tecnológicos (Ver anexo F): Este documento describe el procedimiento que deben seguir los usuarios para llevar a cabo ante el área de tecnología la solicitud de recursos tecnológicos, en conjunto con los formatos y pasos que componen la respectiva gestión de dichos elementos.

- R5-P002 Atención mesa de ayuda (Ver anexo H)**:** Este documento describe el procedimiento que debe seguir el área de tecnología para llevar a cabo el seguimiento, clasificación y desarrollo a cada uno de los requerimientos planteados en la plataforma de mesa de ayuda.

- R5-P003 Seguimiento de recursos tecnológicos (Ver anexo D): Este documento describe claramente el procedimiento que debe seguir el área de tecnología para

llevar a cabo el control, almacenamiento, clasificación y administración de los recursos tecnológicos de Combustibles Líquidos de Colombia S.A. ESP.

- R5-P004 Procedimiento creación hojas de vida de equipos (Ver anexo C): Este documento describe claramente el procedimiento que debe seguir el área de tecnología para realizar la creación, alimentación, actualización y administración de las hojas de vida de los equipos tecnológicos, tales como, Desktop y Laptop de Combustibles Líquidos de Colombia S.A. ESP.

El proceso de tecnología cuenta también con los siguientes formatos codificados en el sistema de gestión de calidad que permiten el correcto funcionamiento de los procedimientos comentados anteriormente, dichos Formatos son:

- R5-F001 Formato solicitud de recursos tecnológicos (Ver anexo P)
- R5-F002 Formato ficha técnica y hoja de vida de equipos (Ver anexo O).
- R5-F003 Acta de entrega recursos tecnológicos (Ver anexo N).
- R5-F004 Acta de devolución recursos tecnológicos (Ver anexo M).
- R5-F005 Formato changes (Ver anexo L).
- R5-F006 Planilla de inventario activos físicos IT (Ver anexo K).
- R5-F007 Seguimiento de software (Ver anexo J).
- R6-F019 Ficha asistencia-tema Capacitación.

Dichos procesos son auditados semestralmente por el área de calidad, las cuales permiten identificar a qué punto se da conformidad a la ejecución de cada procedimiento con lo no con los documentos establecidos y aprobados por la alta gerencia.

3.2 SISTEMAS DE INFORMACIÓN

- ERP - Sistema UNO Versión 8.5 Release 15.06, montado en un servidor Linux Centos, sistema desarrollado en Cobol, el proveedor del sistema es SIESA, se compone por el modulo financiero, comercial, nomina directa y activos fijos.

- En este sistema se lleva a cabo todos los registros contables, nómina y de inventarios.

- CRM - Sales Force, Plataforma web en la nube, en este se lleva a cabo todo el seguimiento a los clientes, se tiene un módulo en donde se le hace seguimiento a la nómina tanto de temporales, como directa, también se tiene un módulo en el que se tienen registrados los inventarios de equipos tecnológicos, un módulo para el registro y seguimiento de helpdesk del área de tecnología, un módulo en el que se lleva a cabo la georreferenciación de los vehículos de la compañía.

- Saasmaint, Plataforma web en la nube, en esta se lleva a cabo el seguimiento al mantenimiento vehicular de la compañía, en el que se tiene un proceso de aprobación de órdenes de compra para los ya mencionados mantenimientos de vehículos.

- B2B, Plataforma web en la que se le hace seguimiento a la ubicación en tiempo real de los vehículos de la compañía (GPS)

- ArcGis, plataforma para llevar a cabo la georreferenciación de clientes

- Plataforma de correos de Google (correos, sites y drive).

- QlikView, Sistema gestor de bases de datos, el cual conecta la información del ERP con la del CRM

- Asterisk, Plataforma local para el tema de Voz Ip, montado en servidor físico bajo sistema operativo linux y al que se accede vía web.

- UTM - Firewall Dell NSA 2400, equipo en el que se lleva a cabo todo el seguimiento de seguridad perimetral de la compañía.

- Servidor de dominio, en este equipo se tiene configurado DHCP y directorio activo (usuarios de la red).

3.3 SERVICIOS DEL ÁREA DE TECNOLOGÍA

- Servicio de soporte en todas las aplicaciones de la compañía.

- Análisis, monitoreo y actualización de la infraestructura tecnológica de la compañía.

- Proveer todos los recursos tecnológicos a los usuarios que en función de su cargo lo requieran.

- Velar por la disponibilidad, integridad y seguridad de las aplicaciones de la compañía.

- Seguimiento a todo el inventario tecnológico de la compañía.

3.4 ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN

Con el fin de determinar el nivel de cumplimiento de los dominios, objetivos de control y controles de seguridad requeridos por el estándar. En el Cuadro 5 se describe el estado actual de conformidad con el Anexo A del estándar ISO/IEC 27001:2013:

Cuadro 5. Estado actual de la seguridad de la información

<table>
<tr><td colspan="4">A.5 Políticas de seguridad de la información</td></tr>
<tr><td colspan="4">A.5.1 Orientación de la dirección para la gestión de la seguridad de la información</td></tr>
<tr><td colspan="4">Objetivo: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.</td></tr>
<tr><td>A.5.1.1</td><td>Políticas para la seguridad de la información.</td><td>Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada
a los empleados y partes externas pertinentes.</td><td>Implementado
SI | NO | PARCIALMENTE
El proceso de tecnología solo cuenta con una política de uso de recurso tecnológico – Política de uso de recurso tecnológico (Ver anexo 2) - y aunque dicha política nombre en algunos de sus ítems la seguridad en los equipos tecnológicos no se encuentra netamente orientada a la seguridad de la información. El proceso de tecnología No cuenta con una política de seguridad de la información definida.</td></tr>
<tr><td>A.5.1.2</td><td>Revisión de la política de seguridad de la información.</td><td>Control: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos,
para asegurar su conveniencia, adecuación y eficacia continúas.</td><td>Implementado
SI | NO | PARCIALMENTE
Teniendo en cuenta lo visto en el ítem A.5.1.1 el proceso de tecnología de Combustibles Líquidos de Colombia S.A. ESP no lleva a cabo revisiones periódicas a la política de seguridad de la información, ya que no se tiene definida dicha política.</td></tr>
</table>

Cuadro 5. (Continuación)

A.6 Organización de la seguridad de la información			
6.1 Organización interna			
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.			
A.6.1.1	Roles y responsabilidades para la seguridad de información.	Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.	Implementado SI / NO / **PARCIALMENTE** Dentro del proceso de tecnología se encuentra definido entre el director y coordinador de tecnología responsabilidades que en términos generales se orientan a la seguridad de la información (Ver 4.4 Situación actual - Funciones del director y coordinador de tecnología), pero no se encuentran definidas responsabilidades y roles claros y específicos dentro del procesos de tecnología de Combustibles Líquidos de Colombia S.A. ESP.
A.6.1.2	Separación de deberes.	Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	Implementado SI / **NO** / PARCIALMENTE En el proceso de tecnología de Combustibles Líquidos de Colombia S.A. ESP NO se lleva a cabo la separación de deberes.
A.6.1.3	Contacto con las autoridades.	Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes.	Implementado SI / **NO** / PARCIALMENTE No se mantienen los contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especial.	Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	Implementado SI / **NO** / PARCIALMENTE No se mantienen contactos apropiados con grupos de interés.

Cuadro 5. (Continuación)

A.6 Organización de la seguridad de la información			
6.1 Organización interna			
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.			
A.6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.	Implementado SI **NO** PARCIALMENTE La seguridad de la información no es prioridad en la gestión de proyectos gestionados.
6.2 Dispositivos móviles y teletrabajo			
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.			
A.6.2.1	Política para dispositivos móviles.	Control: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	Implementado SI **NO** PARCIALMENTE No se cuenta con una política para dispositivos móviles.
A.6.2.2	Teletrabajo.	Control: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo	Implementado SI **NO** PARCIALMENTE No se tiene implementado política para el teletrabajo.
A.7 Seguridad de los recursos humanos			
7.1 Antes de asumir el empleo			
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.			
A.7.1.1	Selección.	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información que se va a tener acceso, y a los riesgos percibidos.	Implementado SI **NO** PARCIALMENTE Teniendo en cuenta que en proceso de tecnología de Combustibles Líquidos de Colombia SA ESP no se ha llevado una clasificación de activos de información ni su respectivo análisis de riesgos no se lleva a cabo la verificación en la selección del personal en función de la clasificación de la información y sus riesgos.

Cuadro 5. (Continuación)

<table>
<tr><td colspan="4">A.7 Seguridad de los recursos humanos</td></tr>
<tr><td colspan="4">7.1 Antes de asumir el empleo</td></tr>
<tr><td colspan="4">Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.</td></tr>
<tr><td>A.7.1.2</td><td>Términos y condiciones del
empleo.</td><td>Control: Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.</td><td>Implementado
SI | NO | PARCIALMENTE
Actualmente Combustibles Líquidos de Colombia S.A. ESP posee dentro de los contratos laborales a los empleados un acuerdo de confidencialidad y un acuerdo de dirección y confianza, pero no se encuentran definidas de forma tal como lo indica el control A.7.1.2.</td></tr>
<tr><td colspan="4">7.2 Durante la ejecución del empleo</td></tr>
<tr><td colspan="4">Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.</td></tr>
<tr><td>A.7.2.1</td><td>Responsabilidades de la dirección.</td><td>Control: La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.</td><td>Implementado
SI | NO | PARCIALMENTE
No se tiene implementado.</td></tr>
<tr><td>A.7.2.2</td><td>Toma de conciencia, educación y formación en la seguridad de la información.</td><td>Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo</td><td>Implementado
SI | NO | PARCIALMENTE
Aunque el área de tecnología lleve a cabo él envió de información que concientice a los usuarios con respecto a la seguridad de información No se llevan a cabo campañas de formación y actualización.</td></tr>
</table>

Cuadro 5. (Continuación)

7.2 Durante la ejecución del empleo			
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.			
A.7.2.3	Proceso disciplinario	Control: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	Implementado SI **NO** PARCIALMENTE No se cuenta con un proceso disciplinario documentado.
7.3 Terminación o cambio de empleo			
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.			
A.7.3.1	Terminación o cambio de responsabilidades de empleo.	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.	Implementado **SI** NO PARCIALMENTE Cada que se presenta un cambio de cargo, reemplazo o finalización de un contrato se lleva a cabo la validación del acceso a la información de la persona que presenta dicho cambio de responsabilidades.
A.8 Gestión de activos			
8.1 Responsabilidad por los activos			
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.			
A.8.1.1	Inventario de activos.	Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.	Implementado **SI** NO PARCIALMENTE Se tiene un inventario de los activos de información de forma básica.

Cuadro 5. (Continuación)

A.8 Gestión de activos			
8.1 Responsabilidad por los activos			
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.			
A.8.1.2	Propiedad de los activos.	Control: Los activos mantenidos en el inventario deberían tener un propietario.	Implementado **SI** NO PARCIALMENTE Dentro del inventario se observa un campo que indica el responsable y/o propietario del respectivo activo de información.
A.8.1.3	Uso aceptable de los activos.	Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	Implementado **SI** NO PARCIALMENTE Se cuenta con una política de uso de recurso tecnológico que indica el uso adecuado y permitido de los activos tecnológicos y de información de Combustibles Líquidos de Colombia S.A. ESP.
A.8.1.4	Devolución de activos.	Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	Implementado **SI** NO PARCIALMENTE Se tiene implementado un procedimiento para la devolución de equipos tecnológicos y de información a través de formato autorizado por el sistema de gestión de calidad implementado en Combustibles Líquidos de Colombia S.A. ESP.

Cuadro 5. (Continuación)

8.2 Clasificación de la información			
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.			
A.8.2.1	Clasificación de la información.	Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	Implementado SI **NO** PARCIALMENTE No se clasifica la información como lo indica el control.
A.8.2.2	Etiquetado de la información.	Control: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Implementado SI **NO** PARCIALMENTE No se etiqueta la información en función de su clasificación.
A.8.2.3	Manejo de activos.	Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Implementado SI **NO** PARCIALMENTE No se cuenta con procedimientos de manejo de activos en función de la clasificación de la información.
8.3 Manejo de medios			
Objetivo: Evitar la divulgación, modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.			
A.8.3.1	Gestión de medios removibles.	Control: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	Implementado SI **NO** PARCIALMENTE No se tienen implementados procedimientos para los medios removibles.
A.8.3.2	Disposición de los medios.	Control: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	Implementado **SI** NO PARCIALMENTE Se cuenta con un procedimiento para la disposición final de equipos tecnológicos.
A.8.3.3	Transferencia de medios físicos.	Control: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	Implementado SI **NO** PARCIALMENTE No se cuentan con procedimientos que aseguren el acceso no autorizado a los medios durante su transporte.

Cuadro 5. (Continuación)

A.9 Control de acceso			
9.1 Requisitos del negocio para control de acceso			
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.			
A.9.1.1	Política de control de acceso.	Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	Implementado SI **NO** PARCIALMENTE No se cuenta con una política para el control de acceso.
A.9.1.2	Política sobre el uso de los servicios de red.	Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	Implementado SI NO **PARCIALMENTE** Se tiene configurada una política de acceso a servicios de red y navegación en el Firewall de la compañía, mas no se tiene documentado.
9.2 Gestión de acceso de usuarios			
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.			
A.9.2.1	Registro y cancelación del registro de usuarios.	Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	Implementado **SI** NO PARCIALMENTE Se cuenta con un software que lleva a cabo el registro y cancelación de acceso de los usuarios, así mismo se administran los derechos de acceso.
A.9.2.2	Suministro de acceso de usuarios.	Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	Implementado SI **NO** PARCIALMENTE No hay un proceso que defina formalmente el acceso de los usuarios a los sistemas, puesto que estos son definidos según sus funciones y su cargo.
A.9.2.3	Gestión de derechos de acceso privilegiado.	Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.	Implementado **SI** NO PARCIALMENTE Se lleva a cabo los procedimientos necesarios para limitar el acceso a los sistemas a través del perfilamiento de los cargos.
A.9.2.4	Gestión de información de autenticación secreta de usuarios.	Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.	Implementado SI **NO** PARCIALMENTE No se cuenta con el proceso de gestión formal.

Cuadro 5. (Continuación)

9.2 Gestión de acceso de usuarios			
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios			
A.9.2.5	Revisión de los derechos de acceso de usuarios.	Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.	Implementado SI **NO** PARCIALMENTE No se lleva a cabo la revisión periódica de los derechos de usuarios.
A.9.2.6	Retiro o ajuste de los derechos de acceso.	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.	Implementado **SI** NO PARCIALMENTE Se llevan a cabo los respectivos cambios de acceso a los sistemas de información cada que hay un retiro o cambio.
9.3 Responsabilidades de los usuarios			
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.			
A.9.3.1	Uso de la información de autenticación secreta.	Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	Implementado **SI** NO PARCIALMENTE A través de la política de uso de recurso tecnológico y de las configuraciones de los diferentes sistemas se les exige a los usuarios la respectiva autenticación a los sistemas de información.
9.4 Control de acceso a sistemas y aplicaciones			
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones			
A.9.4.1	Restricción de acceso Información.	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.	Implementado SI **NO** PARCIALMENTE Teniendo en cuenta que no existe la política de control de acceso no se lleva a cabo el control A.9.4.1
A.9.4.2	Procedimiento de ingreso seguro.	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.	Implementado SI **NO** PARCIALMENTE Teniendo en cuenta que no existe la política de control de acceso no se lleva a cabo el control A.9.4.2

Cuadro 5. (Continuación)

9.4 Control de acceso a sistemas y aplicaciones			
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones			
A.9.4.3	Sistema de gestión de contraseñas.	Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.	Implementado SI **NO** PARCIALMENTE Las aplicaciones corporativas cuentan con su sistema gestor de contraseñas, en el que se exige un minino de características en las contraseñas
A.9.4.4	Uso de programas utilitarios privilegiados	Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.	Implementado SI **NO** PARCIALMENTE No se lleva a cabo la restricción a utilitarios
A.9.4.5	Control de acceso a códigos fuente de programas.	Control: Se debería restringir el acceso a los códigos fuente de los programas.	Implementado **SI** NO PARCIALMENTE Si se tiene restringido el acceso a los códigos fuente de las aplicaciones corporativas.
A.10 Criptografía			
10.1 Controles criptográficos			
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.			
A.10.1.1	Política sobre el uso de controles criptográficos.	Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	Implementado SI **NO** PARCIALMENTE No existe la política de controles criptográficos.

Cuadro 5. (Continuación)

A.10 Criptografía			
10.1 Controles criptográficos			
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.			
A.10.1.2	Gestión de llaves.	Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.	Implementado SI **NO** PARCIALMENTE No existe política para la gestión de llaves criptográficas.
A.11 Seguridad física y del entorno			
11.1 Áreas seguras			
Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.			
A.11.1.1	Perímetro de seguridad física.	Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.	Implementado **SI** NO PARCIALMENTE Se tienen definidos perímetros de seguridad en instalaciones de manejo de información.
A.11.1.2	Controles físicos de entrada.	Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado	Implementado **SI** NO PARCIALMENTE Se cuenta con un sistema de control de acceso físico a través de tarjetas de proximidad, en el que se limita el acceso a ciertos perímetros de la compañía.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones	Implementado **SI** NO PARCIALMENTE Dentro del edificio en el que la compañía desarrolla su actividad administrativa se cuenta con el control de acceso a oficinas y sectores específicos y en oficinas críticas, como gerencia, dirección y entre otras se cuenta con chapas físicas que limitan el acceso a solo el personal autorizado
A.11.1.4	Protección contra amenazas externas y ambientales.	Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Implementado SI **NO** PARCIALMENTE No se cuenta con controles específicos para amenazas extremas y ambientales.

Cuadro 5. (Continuación)

A.11 Seguridad física y del entorno			
11.1 Áreas seguras			
Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.			
A.11.1.5	Trabajo en áreas seguras.	Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.	Implementado **SI** NO PARCIALMENTE La compañía cuenta con procedimientos dentro de su sistema de gestión de calidad de trabajo en áreas seguras.
A.11.1.6	Áreas de despacho y carga.	Control: Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	Implementado **SI** NO PARCIALMENTE Cerca del perímetro en donde se lleva a cabo procesamiento de información no se ejecutan procesos de despacho o carga.
11.2 Equipos			
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.			
A.11.2.1	Ubicación y protección de los equipos.	Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	Implementado **SI** NO PARCIALMENTE Los equipos se encuentran ubicados de forma tal que su acceso sea únicamente para los usuarios autorizados, es decir, ubicados después de los controles de acceso por tarjeta de proximidad y monitoreada por CCTV.
A.11.2.2	Servicios de suministro.	Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Implementado **SI** NO PARCIALMENTE El edificio administrativo cuenta con un sistema de respaldo eléctrico a través de UPS y planta eléctrica que satisface la perdida de suministro de energía.

Cuadro 5. (Continuación)

<table>
<tr><td colspan="4">11.2 Equipos</td></tr>
<tr><td colspan="4">Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.</td></tr>
<tr><td>A.11.2.3</td><td>Seguridad del cableado.</td><td>Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.</td><td>Implementado
SI | NO | PARCIALMENTE
El cableado de la infraestructura de datos se encuentra certificado y protegido ante su manipulación, interferencia y daño.</td></tr>
<tr><td colspan="4">11.2 Equipos</td></tr>
<tr><td colspan="4">Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.</td></tr>
<tr><td>A.11.2.4</td><td>Mantenimiento de equipos.</td><td>Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.</td><td>Implementado
SI | NO | PARCIALMENTE
Se cuenta con un procedimiento en el que se contempla un cronograma, seguimiento y control al mantenimiento de equipos.</td></tr>
<tr><td>A.11.2.5</td><td>Retiro de activos.</td><td>Control: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.</td><td>Implementado
SI | NO | PARCIALMENTE
Para que se lleve a cabo un cambio en la posición de un equipo se solicita al área de tecnología la respectiva autorización, en donde se decide si el usuario se encuentra en la capacidad de hacer el cambio o si el área de tecnología ejecute el cambio.</td></tr>
<tr><td>A.11.2.6</td><td>Seguridad de equipos y activos fuera de las instalaciones.</td><td>Control: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.</td><td>Implementado
SI | NO | PARCIALMENTE
En equipos que se encuentran fuera de las instalaciones se les lleva a cabo configuraciones a nivel de antivirus únicamente.</td></tr>
</table>

Cuadro 5. (Continuación)

11.2 Equipos			
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.			
A.11.2.7	Disposición segura o reutilización de equipos.	Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.	Implementado **SI** NO PARCIALMENTE Cada que se da disposición a los equipos de cómputo se lleva a cabo un proceso de "formateo" que cuenta con reinstalación del sistema operativo y todas las aplicaciones autorizadas por la compañía.
A.11.2.8	Equipos de usuario desatendidos.	Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.	Implementado SI **NO** PARCIALMENTE No se cuenta con procedimientos para los equipos de usuarios desatendidos.
A.11.2.9	Política de escritorio limpio y pantalla limpia.	Control: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información	Implementado SI **NO** PARCIALMENTE No se tiene adoptada una política de escritorio limpio.
A.12 Seguridad de las operaciones			
12.1 Procedimientos operacionales y responsabilidades			
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.			
A.12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten	Implementado SI **NO** PARCIALMENTE Los procedimientos de operación no se documentan, ni se ponen a disposición de los usuarios
A.12.1.2	Gestión de cambios	Control: Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información	Implementado **SI** NO PARCIALMENTE Cada que se presenta un cambio en la infraestructura tecnológica se lleva a cabo la documentación del cambio a través del formato autorizado por el sistema de gestión de calidad.

Cuadro 5. (Continuación)

<table>
<tr><td colspan="4">A.12 Seguridad de las operaciones</td></tr>
<tr><td colspan="4">12.1 Procedimientos operacionales y responsabilidades</td></tr>
<tr><td colspan="4">Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.</td></tr>
<tr><td>A.12.1.3</td><td>Gestión de capacidad</td><td>Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.</td><td>Implementado
SI | NO | PARCIALMENTE
No se lleva a cabo control periódico de capacidad.</td></tr>
<tr><td>A.12.1.4</td><td>Separación de los ambientes de desarrollo, pruebas y operación</td><td>Control: Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.</td><td>Implementado
SI | NO | PARCIALMENTE
En la aplicación ERP (aplicación en la que se lleva control de la operación) se tiene un ambiente de pruebas en el que se llevan a cabo las ya mencionadas pruebas antes de ponerlas en producción.</td></tr>
<tr><td colspan="4">12.2 Protección contra códigos maliciosos</td></tr>
<tr><td colspan="4">Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.</td></tr>
<tr><td>A.12.2.1</td><td>Controles contra códigos maliciosos.</td><td>Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.</td><td>Implementado
SI | NO | PARCIALMENTE
Se tiene implementado un sistema de seguridad a través de una UTM, que contiene un firewall, un sistema de detección y prevención a intrusos, junto con un sistema antivirus, que se convierten en un control de código malicioso.</td></tr>
<tr><td colspan="4">12.3 Copias de respaldo</td></tr>
<tr><td colspan="4">Objetivo: Proteger contra la perdida de datos</td></tr>
<tr><td>A.12.3.1</td><td>Respaldo de información.</td><td>Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.</td><td>Implementado
SI | NO | PARCIALMENTE
Se lleva a cabo copia de seguridad de la información de usuarios y servidores, pero no se tiene implementado la copia de las imágenes de los mismos que permitan una rápida recuperación en caso de desastre.</td></tr>
</table>

Cuadro 5. (Continuación)

12.4 Registro y seguimiento			
Objetivo: Registrar eventos y generar evidencia			
A.12.4.1	1 Registro de eventos.	Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	Implementado SI **NO** PARCIALMENTE No se lleva a cabo el registro de eventos de los usuarios, más que eventos de seguridad en el log del Firewall.
A.12.4.2	Protección de la información de registro.	Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.	Implementado SI **NO** PARCIALMENTE No se ejecuta el control A.12.4.2
A.12.4.3	Registros del administrador y del operador.	Control: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.	Implementado SI **NO** PARCIALMENTE No se lleva a cabo el registro.
12.4 Registro y seguimiento			
Objetivo: Registrar eventos y generar evidencia			
A.12.4.4	Sincronización de relojes.	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.	Implementado **SI** NO PARCIALMENTE Se hace la respectiva configuración en el servidor de dominio y directorio activo para que a través de este se configuración se sincronice una única hora en todos los equipos de cómputo de la red.
12.5 Control de software operacional			
Objetivo: Asegurar la integridad de los sistemas operacionales.			
A.12.5.1	Instalación de software en sistemas operativos.	Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.	Implementado SI **NO** PARCIALMENTE Dentro de la política de uso de recurso tecnológico se menciona la exigencia al usuario de no instalar software autorizado, pero no se tiene un procedimiento implementado para controlar esto.

Cuadro 5. (Continuación)

12.6 Gestión de la vulnerabilidad técnica			
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas			
A.12.6.1	Gestión de las vulnerabilidades técnicas.	Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Implementado SI **NO** PARCIALMENTE No se lleva a cabo la gestión de vulnerabilidades técnicas.
A.12.6.2	Restricciones sobre la instalación de software.	Control: Restricciones sobre la instalación de software.	Implementado **SI** NO PARCIALMENTE Se cuenta con una restricción para la instalación de software, en el que el sistema operativa solicita por obligatoriedad la contraseña del administrador para ejecutar la instalación, en donde dicha contraseña solo la tiene el área de tecnología.
12.7 Consideraciones sobre auditorias de sistemas de información			
Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.			
A.12.7.1	Información controles de auditoría de sistemas	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	Implementado SI **NO** PARCIALMENTE No se ejecutan auditorías a los sistemas de información.
13. Seguridad de las comunicaciones			
13.1 Gestión de la seguridad de las redes			
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte			
A.13.1.1	Controles de redes.	Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.	Implementado **SI** NO PARCIALMENTE Se gestiona a través de firewall, IDS e IPS controles sobre la red.

Cuadro 5 (Continuación)

13.1 Gestión de la seguridad de las redes			
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.			
A.13.1.2	Seguridad de los servicios de red.	Control: Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	Implementado SI **NO** PARCIALMENTE No se tiene implementado el control de seguridad en los servicios de red.
A.13.1.3	Separación en las redes.	Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.	Implementado **SI** NO PARCIALMENTE Se tiene segmentada la red en subredes.
13.2 Transferencia de información			
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa			
A.13.2.1	Políticas y procedimientos de transferencia de información.	Control: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.	Implementado SI **NO** PARCIALMENTE No se tiene implementada una política de transferencia de información.
13.2 Transferencia de información			
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa			
A.13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.	Implementado SI **NO** PARCIALMENTE No se tienen acuerdos de transferencia de información.
A.13.2.3	Mensajería electrónica	Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.	Implementado SI **NO** PARCIALMENTE No se tienen procesos que lleven a cabo la protección a la mensajería electrónica, excepto de la ofrecida por el proveedor (google).

Cuadro 5. (Continuación)

<table>
<tr><td colspan="4">13.2 Transferencia de información</td></tr>
<tr><td colspan="4">Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa</td></tr>
<tr><td>A.13.2.4</td><td>Acuerdos de confidencialidad o de no divulgación.</td><td>Control: Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.</td><td>Implementado
SI | NO | PARCIALMENTE
Se cuentan con acuerdos de confidencialidad entre los empleados y los terceros externos.</td></tr>
<tr><td colspan="4">14 Adquisición, desarrollo y mantenimientos de sistemas</td></tr>
<tr><td colspan="4">14.1 Requisitos de seguridad de los sistemas de información</td></tr>
<tr><td colspan="4">Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.</td></tr>
<tr><td>A.14.1.1</td><td>Análisis y especificación de requisitos de seguridad de la información</td><td>Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes</td><td>Implementado
SI | NO | PARCIALMENTE
No se lleva a cabo el respectivo análisis y especificación de los requisitos de seguridad de la información para los nuevos sistemas.</td></tr>
<tr><td>A.14.1.2</td><td>Seguridad de servicios de las aplicaciones en redes publicas</td><td>Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas</td><td>Implementado
SI | NO | PARCIALMENTE
No se tiene implementado el control para la seguridad de servicios de las aplicaciones en redes públicas.</td></tr>
</table>

Cuadro 5 (Continuación)

14 Adquisición, desarrollo y mantenimientos de sistemas			
14.1 Requisitos de seguridad de los sistemas de información			
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.			
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada	Implementado SI **NO** PARCIALMENTE No se tiene implementado el control a la protección de transacciones de los servicios de las aplicaciones.
14.2 Seguridad en los procesos de desarrollo y soporte			
Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.			
A.14.2.1	Política de desarrollo seguro.	Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización	Implementado SI **NO** PARCIALMENTE La compañía no lleva a cabo desarrollo de aplicaciones.
A.14.2.2	Procedimientos de control de cambios en sistemas.	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.	Implementado SI **NO** PARCIALMENTE La compañía no lleva a cabo desarrollo de aplicaciones.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación.	Control: Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	Implementado **SI** NO PARCIALMENTE Cada que se ejecutan cambios en las plataformas de la compañía se llevan a cabo las respectivas pruebas técnicas con el fin de validar su funcionamiento eficiente.

Cuadro 5. (Continuación)

14.2 Seguridad en los procesos de desarrollo y soporte			
Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.			
A.14.2.4	Restricciones en los cambios a los paquetes de software.	Control: Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.	Implementado SI **NO** PARCIALMENTE No hay restricción a cambios en el área de tecnología.
14.2 Seguridad en los procesos de desarrollo y soporte			
Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.			
A.14.2.5	Principios de construcción de sistemas seguros.	Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	Implementado SI **NO** PARCIALMENTE No se tienen claros los principios de construcción de sistemas seguros.
A.14.2.6	Ambiente de desarrollo seguro.	Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	Implementado SI **NO** PARCIALMENTE La compañía no lleva a cabo desarrollo de aplicaciones.
A.14.2.7	Desarrollo contratado externamente	Control: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externa mente	Implementado SI **NO** PARCIALMENTE A la actualidad no se ha solicitado desarrollos de software a la medida con terceros externos.
A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.	Implementado SI **NO** PARCIALMENTE La compañía no lleva a cabo desarrollo de aplicaciones.

Cuadro 5. (Continuación)

<table>
<tr><td colspan="4">14.2 Seguridad en los procesos de desarrollo y soporte</td></tr>
<tr><td colspan="4">Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.</td></tr>
<tr><td rowspan="3">A.14.2.9</td><td rowspan="3">Prueba de aceptación de sistemas.</td><td rowspan="3">Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.</td><td>Implementado</td></tr>
<tr><td>SI NO PARCIALMENTE</td></tr>
<tr><td>La compañía no lleva a cabo desarrollo de aplicaciones.</td></tr>
<tr><td colspan="4">14.3 Datos de Prueba</td></tr>
<tr><td colspan="4">Objetivo: Asegurar la protección de los datos usados para pruebas.</td></tr>
<tr><td rowspan="3">A.14.3.1</td><td rowspan="3">Protección de datos de prueba.</td><td rowspan="3">Control: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente</td><td>Implementado</td></tr>
<tr><td>SI NO PARCIALMENTE</td></tr>
<tr><td>La compañía no lleva a cabo desarrollo de aplicaciones.</td></tr>
<tr><td colspan="4">15. Relación con los proveedores</td></tr>
<tr><td colspan="4">15.1 Seguridad de la información en las relaciones con los proveedores</td></tr>
<tr><td colspan="4">Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.</td></tr>
<tr><td rowspan="3">A.15.1.1</td><td rowspan="3">Política de seguridad de la información para las relaciones con proveedores.</td><td rowspan="3">Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar.</td><td>Implementado</td></tr>
<tr><td>SI NO PARCIALMENTE</td></tr>
<tr><td>No se tiene implementado una política de seguridad de la información para las relaciones con proveedores.</td></tr>
<tr><td rowspan="3">A.15.1.2</td><td rowspan="3">Tratamiento de la seguridad dentro de los acuerdos con proveedores.</td><td rowspan="3">Control: Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar almacenar comunicar o suministrar componentes de infraestructura de TI para la información de la organización.</td><td>Implementado</td></tr>
<tr><td>SI NO PARCIALMENTE</td></tr>
<tr><td>No se lleva a cabo tratamiento de la seguridad de la información dentro de los acuerdos con proveedores.</td></tr>
</table>

Cuadro 5. (Continuación)

<table>
<tr><td colspan="4">15. Relación con los proveedores</td></tr>
<tr><td colspan="4">15.1 Seguridad de la información en las relaciones con los proveedores</td></tr>
<tr><td colspan="4">Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.</td></tr>
<tr><td>A.15.1.3</td><td>Cadena de suministro de tecnología de información y comunicación.</td><td>Control: Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.</td><td>Implementado
SI NO PARCIALMENTE
No se cuenta con la cadena de suministro de tecnología de información y comunicación con proveedores.</td></tr>
<tr><td colspan="4">15.2 Gestión de la prestación de servicios con los proveedores</td></tr>
<tr><td colspan="4">Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.</td></tr>
<tr><td>A.15.2.1</td><td>Seguimiento y revisión de los servicios de los proveedores.</td><td>Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.</td><td>Implementado
SI NO PARCIALMENTE
No se lleva a cabo el seguimiento y revisión de los servicios de los proveedores</td></tr>
<tr><td>A.15.2.2</td><td>Gestión de cambios en los servicios de proveedores.</td><td>Control: Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.</td><td>Implementado
SI NO PARCIALMENTE
No existe la gestión de cambios en los servicios con proveedores.
.</td></tr>
</table>

Cuadro 5. (Continuación)

<table>
<tr><td colspan="4">16. Gestión de incidentes de seguridad de la información</td></tr>
<tr><td colspan="4">16.1 Gestión de incidentes y mejoras en la seguridad de la información</td></tr>
<tr><td colspan="4">Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades</td></tr>
<tr><td>A.16.1.1</td><td>Responsabilidad y procedimientos.</td><td>Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.</td><td>Implementado
SI NO PARCIALMENTE
La compañía no cuenta con gestión a incidentes.</td></tr>
<tr><td>A.16.1.2</td><td>Reporte de eventos de seguridad de la información.</td><td>Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.</td><td>Implementado
SI NO PARCIALMENTE
La compañía no cuenta con gestión a incidentes.</td></tr>
<tr><td colspan="4">16. Gestión de incidentes de seguridad de la información</td></tr>
<tr><td colspan="4">16.1 Gestión de incidentes y mejoras en la seguridad de la información</td></tr>
<tr><td colspan="4">Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades</td></tr>
<tr><td>A.16.1.3</td><td>Reporte de debilidades de
seguridad de la información.</td><td>Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.</td><td>Implementado
SI NO PARCIALMENTE
A través de sensibilización se les pide a los usuarios que informen cualquier novedad en cuantas posibles vulnerabilidades.</td></tr>
</table>

Cuadro 5. (Continuación)

16. Gestión de incidentes de seguridad de la información			
16.1 Gestión de incidentes y mejoras en la seguridad de la información			
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades			
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.	Implementado SI **NO** PARCIALMENTE La compañía no cuenta con gestión a incidentes.
A.16.1.5	Respuesta a incidentes de seguridad de la información.	Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	Implementado SI **NO** PARCIALMENTE La compañía no cuenta con gestión a incidentes.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información.	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.	Implementado SI **NO** PARCIALMENTE La compañía no cuenta con gestión a incidentes.
A.16.1.7	Recolección de evidencia.	Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	Implementado SI **NO** PARCIALMENTE La compañía no cuenta con gestión a incidentes.

Cuadro 5. (Continuación)

<table>
<tr><td colspan="4">17 Aspectos de seguridad de la información de la gestión de continuidad de negocio</td></tr>
<tr><td colspan="4">17.1 Continuidad de seguridad de la información</td></tr>
<tr><td colspan="4">Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización</td></tr>
<tr><td>A.17.1.1</td><td>Planificación de la continuidad de la seguridad
de la información.</td><td>Control: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.</td><td>Implementado
SI NO PARCIALMENTE
No se cuenta con una planificación de la continuidad de la seguridad de la información.</td></tr>
<tr><td>A.17.1.2</td><td>Implementación de la continuidad de la seguridad de la información.</td><td>Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.</td><td>Implementado
SI NO PARCIALMENTE
No se tiene implementado la continuidad de la seguridad de la información.</td></tr>
<tr><td>A.17.1.3</td><td>Verificación, revisión y evaluación de la continuidad de la seguridad de la información.</td><td>Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.</td><td>Implementado
SI NO PARCIALMENTE
No se tiene implementado la continuidad de la seguridad de la información.</td></tr>
<tr><td colspan="4">17.2 Redundancias</td></tr>
<tr><td colspan="4">Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.</td></tr>
<tr><td>A.17.2.1</td><td>Disponibilidad de instalaciones de procesamiento de información.</td><td>Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.</td><td>Implementado
SI NO PARCIALMENTE
No se tiene redundancia de la instalación de procesamiento de información.</td></tr>
</table>

Cuadro 5. (Continuación)

18. Cumplimiento			
18.1 Cumplimiento de requisitos legales y contractuales			
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.			
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	Implementado **SI** NO PARCIALMENTE Este proceso lo ejecuta a cabalidad el área jurídica de la compañía.
A.18.1.2	Derechos de propiedad intelectual.	Control: Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	Implementado **SI** NO PARCIALMENTE Se tienen implementados procedimientos para validar que se cumpla a cabalidad la norma de derechos de propiedad intelectual.
A.18.1.3	Protección de registros.	Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	Implementado SI **NO** PARCIALMENTE No se lleva a cabo la protección de registros. **SI** NO PARCIALMENTE Teniendo en cuenta que es una empresa de servicios públicos se tienen implementados procedimientos que permitan el cumplimiento de la norma de privacidad y protección de datos personales.

Cuadro 5. (Continuación)

<table>
<tr><td colspan="4">18. Cumplimiento</td></tr>
<tr><td colspan="4">18.1 Cumplimiento de requisitos legales y contractuales</td></tr>
<tr><td colspan="4">Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.</td></tr>
<tr><td>A.18.1.5</td><td>Reglamentación de controles criptográficos.</td><td>Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.</td><td>Implementado
SI | NO | PARCIALMENTE
No se utilizan controles criptográficos.</td></tr>
<tr><td colspan="4">18.2 Revisiones de seguridad de la información</td></tr>
<tr><td colspan="4">Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.</td></tr>
<tr><td>A.18.2.1</td><td>Revisión independiente de la seguridad de la información.</td><td>Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.</td><td>Implementado
SI | NO | PARCIALMENTE
No se lleva a cabo revisión sobre la gestión de la seguridad de la información.</td></tr>
<tr><td>A.18.2.2</td><td>Cumplimiento con las políticas y normas de seguridad.</td><td>Control: Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.</td><td>Implementado
SI | NO | PARCIALMENTE
Teniendo en cuenta que no se posee una política de seguridad de la información no se valida su cumplimiento.</td></tr>
</table>

Cuadro 5. (Continuación)

<table>
<tr><td colspan="5">18. Cumplimiento</td></tr>
<tr><td colspan="5">18.1 Cumplimiento de requisitos legales y contractuales</td></tr>
<tr><td colspan="5">Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.</td></tr>
<tr><td rowspan="2">A.18.2.3</td><td rowspan="2">Revisión del cumplimiento técnico.</td><td rowspan="2">Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y
normas de seguridad de la información.</td><td>Implementado</td><td>SI NO PARCIALMENTE</td></tr>
<tr><td colspan="2">Teniendo en cuenta que no se posee una política de seguridad de la información no se valida su cumplimiento.</td></tr>
<tr><td colspan="5">Fuente: Autores</td></tr>
</table>

El cuadro 5 permite identificar el estado de la seguridad de la información en Combustibles Líquidos de Colombia, reflejando el avance de cada uno de los dominios, objetivos de control y controles de seguridad requeridos por la norma ISO/IEC 27001:2013, en su Anexo A..

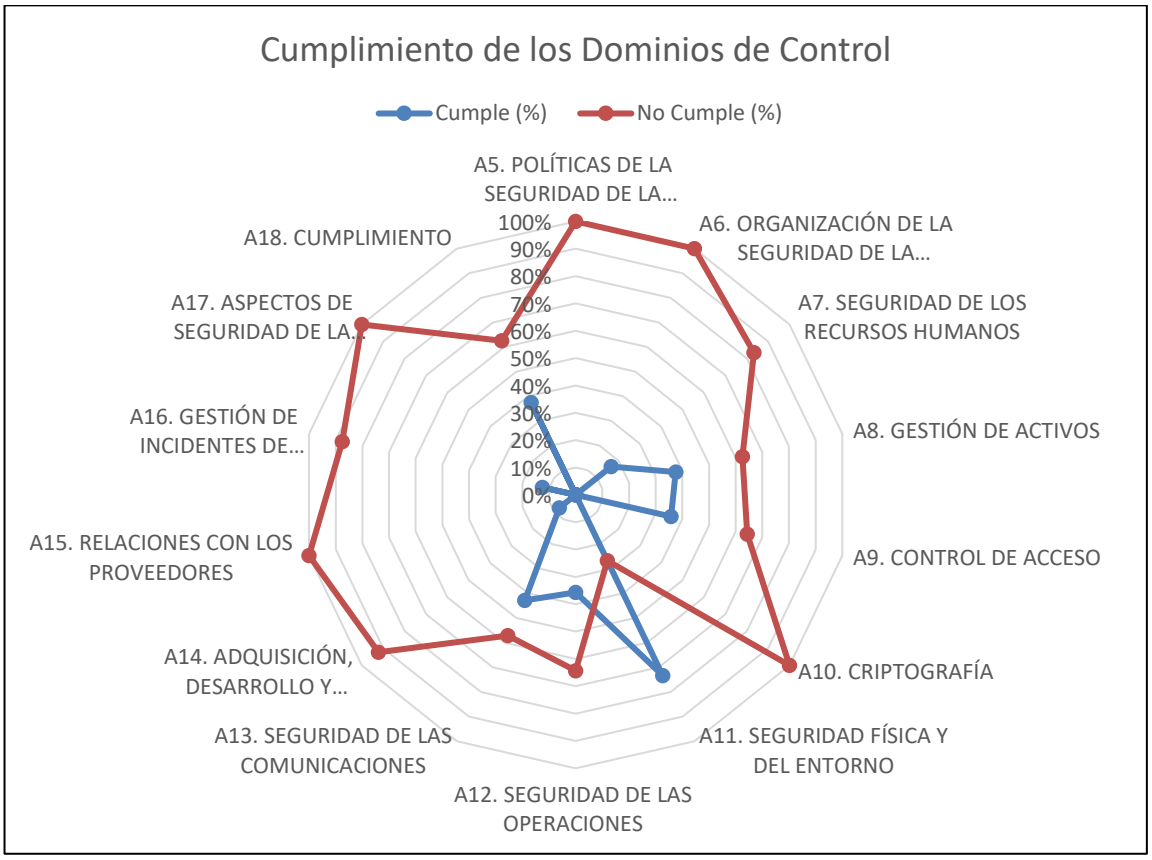
La Tabla 1 se identifica el estado actual de los dominios de control para el que se agrupa por Dominios de control, el nivel de cumplimiento, en donde se toma realiza una estimación de porcentaje de cada control cumplido versus la cantidad de controles requeridos en el dominio. Con el nivel de cumplimiento para cada dominio de control, se puede concluir que en general Combustibles Líquidos de Colombia solo tiene un 21% de cumplimiento, valor que representa los procedimientos y políticas asociados con la seguridad de la información con los que cuenta. Eso quiere decir que no cumple con el 79% de los requisitos de control requeridos para tener un SGSI.

Tabla 1. Estado actual de los dominios de Control

Dominio de control	Cumple (%)	No Cumple (%)
A5. Políticas de la seguridad de la información	0%	100%
A6. Organización de la seguridad de la información	0%	100%
A7. Seguridad de los recursos humanos	16.7%	83.3%
A8. Gestión de activos	37.5%	62.5%
A9. Control de acceso	35.7%	64.3%
A10. Criptografía	0.0%	100.0%
A11. Seguridad física y del entorno	73.3%	26.7%
A12. Seguridad de las operaciones	35.7%	64.3%
A13. Seguridad de las comunicaciones	42.9%	57.1%
A14. Adquisición, desarrollo y mantenimiento de sistemas	7.7%	92.3%
A15. Relaciones con los proveedores	0.0%	100.0%
A16. Gestión de incidentes de seguridad de la información	12.5%	87.5%
A17. Aspectos de seguridad de la información de la gestión de la continuidad del negocio	0.0%	100.0%
A18. Cumplimiento	37.5%	62.5%
Fuente: Autores		

La figura 11 representa gráficamente la tabla 1, en la que se evidencia el estado actual de los dominios de control de forma radial.

Figura11. Análisis de Cumplimiento de los Dominios



Fuente: Autores

A continuación se realizan las siguientes observaciones sobre el estado actual de la seguridad de la información y sobre los controles implementados más relevantes, que hacen parte de las bases del sistema de gestión de seguridad de Combustibles Líquidos de Colombia S.A.:

La alta dirección se encuentra comprometida con la seguridad de la información y reconoce la importancia de la misma.

Dentro del proceso de tecnología de Combustibles Líquidos de Colombia S.A. ESP se lleva a cabo una gestión y administración básica de sus activos tecnológicos, el cual cuenta con procedimientos documentados y reconocidos por la organización, para el desarrollo del proceso.

Aunque se lleve a cabo la administración y control de los activos no existe una valoración formal, ni una matriz de riesgo orientada a estos activos.

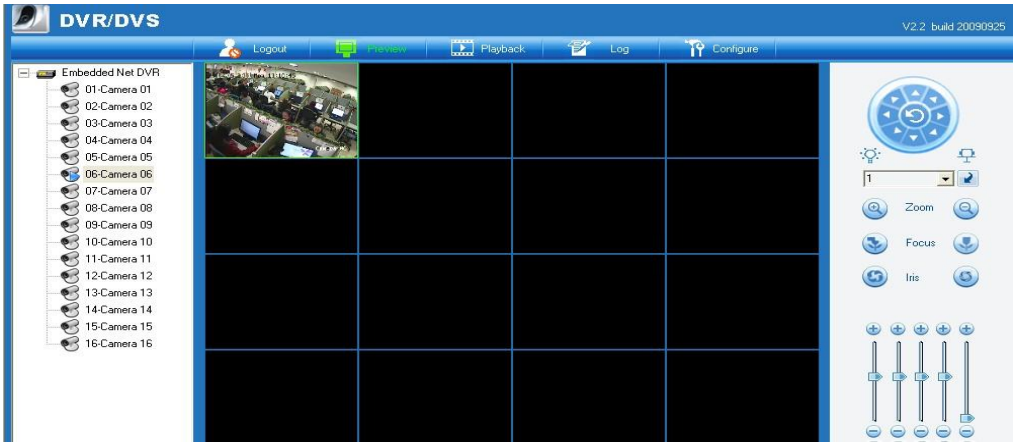
En cuanto a seguridad de información en esa gestión de activos, solo se valida el seguimiento de la ejecución del back up de desktop`s y laptop`s conectados en la sede principal en Bogotá, quedando descubiertas de este procedimiento el resto de áreas.

La compañía cuenta con un sistema de control de acceso conformado por dispositivos o sensores que se activan con tarjetas de proximidad. Dichas tarjetas de proximidad poseen un único número de identificación o id el cual es asignado a un único usuario, a este mismo id se le configura un respectivo perfil de acceso, junto con un perfil de horario de ingreso y salida.

Los dispositivos en conjunto reúnen la información de activación, es decir, alimentan una base de datos con la información de entradas y salidas en cada una de las puertas de la compañía a través de un software llamado KANTECH, el cual permite la administración, configuración y parametrización de las características anteriormente nombradas. El ya mencionado software permite también llevar a cabo el control de las puertas de emergencia, es decir, la activación o desactivación de las alarmas, las cuales permiten una configuración básica en la que permanecen o normalmente abierta o normalmente cerradas.

La compañía también cuenta con un esquema de CCTV o circuito cerrado de televisión, compuesto por 14 cámaras ubicadas estratégicamente en el edificio de la compañía, las cuales son administradas y monitoreadas a través de un dispositivo DVR al cual accede remotamente los agentes de vigilancia (servicio mercerizado con la empresa SECURITAS) en donde el dispositivo DVR almacena hasta 15 días, en donde después de completar el respectivo almacenamiento inicia un proceso de re-escritura. (Ver figura 12)

Figura 12. Controlador del CCTV de Combustibles Líquidos de Colombia S.A. ESP



Fuente: COMBUSTIBLES LÍQUIDOS DE COLOMBIA S.A. ESP. Sistema de Gestión de Calidad. [En línea], [consultado el 25 de abril de 2016]. Disponible en: Combustibles**-líquidos-de-Colombia.**

En cuanto al control de acceso a aplicaciones, Combustibles Líquidos de Colombia S.A. ESP tiene implementado en cada uno de ellas sistemas básicos de autenticación por usuario y contraseña y su respectivo perfilamiento que por orden de la alta gerencia no se nombran en este proyecto.

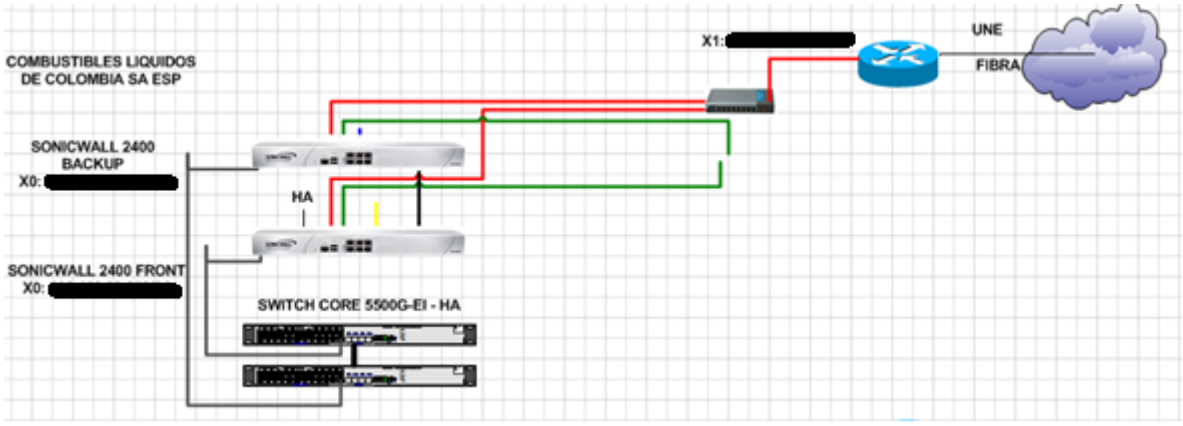
Combustibles Líquidos de Colombia S.A. ESP no tiene implementados procedimientos para el cifrado de información. El único procedimiento que cuenta con cifrado SSL es la conexión por VPN (Virtual Private Network), que cumple con la función de una conexión segura con las otras agencias de Combustibles Líquidos de Colombia S.A. ESP a la sede principal en Bogotá a aplicaciones tales como el Sistema UNO. Dicha conexión VPN se hace a través del Firewall UTM por medio de la herramienta VPNClient.

Como se mencionó en la sección de control de acceso hay un sistema que limita el acceso de personal no autorizado el centro de datos, en donde se almacena toda la información de la compañía, al que solo pueden acceder los integrantes del área de tecnología. Dentro de este control se identifican dos cámaras, una que apunta a la puerta del centro de datos y una al interior del centro de datos, las cuales graban las 24 horas del día los 7 días a la semana a través de un DVR que almacena en discos duros.

En cuanto a la seguridad de redes de la compañía se cuenta con un dispositivo UTM, en el que reúne las características de Firewall, IDS, IPS, antivirus y entre otros, el cual es ubicado estratégicamente en la red para el cumplimiento de sus respectivas funciones. En dicho dispositivo se lleva a cabo filtrado de contenido,

configuración de políticas de navegación, control de puertos, conexiones por VPN, NAT, consumo de canal y entre otras operaciones que permiten dar un grado de seguridad a la red, incluyendo también que este dispositivo se encuentra configurado en HA o alta disponibilidad en donde tiene un dispositivo exactamente igual que al presentarse alguna falla en el activo, este entra en estado pasivo y el secundario en activo: (Ver figura 13)

Figura 13 . Diagrama de seguridad perimetral de Combustibles Líquidos de Colombia S.A. ESP



Fuente: COMBUSTIBLES LÍQUIDOS DE COLOMBIA S.A. ESP. Sistema de Gestión de Calidad. [En línea], [consultado el 25 de abril de 2016]. Disponible en: Combustibles-**LÍQUIDOS-de-Colombia.**

La compañía cuenta con un sistema de control de incendio compuesto por 80 sensores de humo y un panel principal, al cual no se le hace un mantenimiento periódico aproximadamente desde hace un año.

Combustibles Líquidos de Colombia S.A. ESP cuenta también con un sistema de aire acondicionado compuesto por un aspersor ubicado en el cuarto eléctrico y un equipo compuesto por condensadora y controlador de aire que trabaja con gas refrigerante y el cual se encuentra ubicado en el data center, en donde permanece a una temperatura de 17°C.

Todo el anterior esquema descrito permite proteger físicamente daños a equipos o dispositivos que almacenan información de todas las categorías de Combustibles Líquidos de Colombia S.A. ESP.

La compañía también cuenta con un esquema de transferencia eléctrica caracterizado y compuesto por una planta eléctrica diésel que soporta todo la electricidad del edificio completo con una autonomía dependiente a la cantidad de combustible que tenga en su respectivo tanque, este también es apoyada por una

UPS de 15 KVA que cubre únicamente los equipos y dispositivos ubicados en el data center por una autonomía de 4 horas.
Combustibles Líquidos de Colombia S.A. ESP cuenta con un sistema de Back Up en la sede administrativa, el cual utiliza una herramienta gratuita que transfiere la información prioridad de los usuarios a un servidor con discos duros externos (Esta tarea solo se lleva a cabo en los servidores y en los usuarios de la sede administrativa, en los usuarios externos no se lleva a cabo la ejecución de un Back Up periódico).

Combustibles Líquidos de Colombia S.A. ESP cuenta con una sola aplicación en ambiente de pruebas, el cual corresponde al Sistema UNO, en el que se hacen pruebas antes de actualizaciones, configuraciones y mantenimientos. Esta versión de prueba contiene la misma base de datos que el sistema original y al que solo tienen acceso los integrantes del área de tecnología. No se tiene implementados controles de seguridad a este ambiente de pruebas excepto por el control de acceso por usuario y contraseña, el cual solo tiene un usuario máster con acceso a todos los módulos de la aplicación, dicho usuario es administrado por el área de tecnología.

4. ACTIVOS DE INFORMACIÓN

De acuerdo con los lineamientos establecidos en la norma ISO 27001:2013, los activos de información deben ser identificados y se debe definir las responsabilidades de protección apropiadas, lo cual implica valorarlos de acuerdo con su disponibilidad, confidencialidad e integridad.

Se denomina activo de información, a aquello que tiene algún valor para la organización y por tanto este debe protegerse.

Cada activo de información debe contar con dos (2) características principales:

- Responsabilidad por los activos: Se debe definir un responsable por cada activo de información. El objetivo es, Identificar los activos de información de la entidad y elaborar el inventario de activos, manteniendo la propiedad, uso aceptable y devolución.

- Clasificación de la Información: Se debe Asegurar que los activos de información reciban un nivel apropiado de protección, de acuerdo con el nivel de criticidad e importancia, clasificación etiquetado y manejo de los activos.

4.1 IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

Para la identificación y clasificación de los activos de información, se requiere la participación del líder del proceso del área de tecnología, el cual identifica con los responsables de los activos, cuáles y cuantos activos de información tienen bajo su responsabilidad. En este proceso de Identificación pueden participar personas del área de direccionamiento estratégico y gestión documental entre otros.

4.1.1 Tipos de activos de información. Los siguientes son los tipos de activos de información que se deben tener en cuenta en el proceso de valoración de activos del proceso de tecnología en Combustibles Líquidos de Colombia S.A. ESP:

- Información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad y contingencia, información archivada, etc.

- Software: El software que se utiliza para la gestión de la información (sistema operativo, aplicativos, base de datos, ofimática-documentos electrónicos), software de aplicaciones, herramientas de desarrollo y publicación de contenidos, utilitarios, etc.

- Tecnología: Es todo el hardware donde se maneje la información y las comunicaciones.

.

- Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PABXs, máquinas de fax, contestadores automáticos, switches de datos, etc.), medios magnéticos (cintas, discos, dispositivos móviles de almacenamiento de datos – pen drives, discos externos, etc.-), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado, controles automatizados de acceso, etc.), mobiliario, lugares de emplazamiento, etc.

- Servicios: servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).Aquí se consideran tanto los servicios internos, aquellos que una parte de la organización suministra a otra (por ejemplo la gestión administrativa), como los externos, aquellos que la organización suministra a clientes y usuarios (por ejemplo la comercialización de productos). Soportado por plataformas de google drive, de internet, portales web, canales, FTPs, data center, agentes de configuración tecnológico o por prestación de un servicio de un proveedor o contratista.

- Recurso humano: es decir de carácter no monetario y sin apariencia física (conocimiento del personal, marcas, patentes, know how, licencias, concesiones, franquicias). En esta categoría se encuentra tanto el personal propio de la organización, como el personal subcontratado, los clientes, usuarios y, en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la organización.

Los activos identificados que hacen parte del proceso de gestión de tecnología en Combustibles Líquidos de Colombia se muestran en el cuadro 6, en el que se visualiza el nombre del activo y su respectiva descripción

Cuadro 6. Activos de Información

Nombre Activo	Descripción
Manuales y procedimientos	Manuales y procedimientos del proceso de gestión de operaciones de IT, en las que se describen y caracterizan el proceso "R12-F004 Caracterización de Procesos", instructivos de ejecución de procedimientos específicos sobre elementos y aplicaciones del proceso de IT "R5-I001 Instructivo Respaldo de Información de Estaciones de Trabajo", formatos para control y seguimiento de la operación: "R5-F001 Formato Solicitud de Recursos Tecnológicos", "R5-F002 Formato Ficha Técnica y Hoja de Vida de Equipos", "R5-F005 Formato Changes", "R5-F006 Planilla de Inventario Activos físicos", "R5-F007 Seguimiento de Software"
Contratos	Contratos con proveedores de comunicaciones y aplicaciones, para las que se tienen en cuenta clausulas jurídicas a las que haya lugar según el tipo de contrato, tales como, cláusulas de permanencia, de confidencialidad, de penalidad y costos.
Bases de datos	**CG1:** Base de datos de información contable, financiera, comercial y nomina, desarrollada en lenguaje cobol, almacenada en un servidor virtual con sistema operativo Linux Centos, al que se accede únicamente a través de la aplicación "Sistema UNO Versión 8.5 Release 1502". **SalesForce:** Base de datos de información de clientes, funcionarios, novedades de nómina, equipos tecnológicos, georreferenciación y call center, almacenada en la nube y resguardado en varios datacenters a nivel mundial por el proveedor de la aplicación, accedido por web a través del perfilamiento de usuarios. **SaasMaint:** Base de datos de información de vehículos y todo su proceso de mantenimiento, almacenada en la nube y resguardado en varios datacenters a nivel mundial por el proveedor de la aplicación, accedido por web a través del perfilamiento de usuarios. **MySQL (Biable):** Base de datos con toda la información de la aplicación "Sistema UNO Ver. 8.5 Release 1502" utilizada para la extracción y análisis de información de dicha aplicación, almacenada en servidor virtual con sistema operativo Linux Centos.
Actas	Actas de Entregas y Actas de Devolución tanto con usuarios, como con proveedores "R5-F003 Acta de Entrega Recursos Tecnológicos", "R5-F004 Acta de Devolución Recursos Tecnológicos".
Informes	Informes de Gestión e Informes de Operación generados mensualmente para análisis de la alta dirección, tales como, indicadores de gestión, estado del presupuesto asignado, control de costos y gastos, seguimiento y control de comunicaciones e informes de calidad de Help Desk.
Equipo de gestión de operaciones TI	Personal encargado de la gestión de Operaciones de IT (Dirección de Tecnología, Coordinación Tecnología y auxiliar de tecnología)

Cuadro 6. (Continuación)

Nombre Activo	Descripción
Data Center	Lugar en el que se ubican la Granja de Servidores, Infraestructura de comunicaciones, CCTV, Control de acceso, Aire acondicionado
Aplicaciones core	Aplicaciones críticas para la operación del negocio, tales como, Sistema UNO CG1: Aplicación desarrollada en cobol por el proveedor SIESA, instalada en un servidor virtual con sistema operativo Linux Centos, compuesto por 4 módulos principales (financiero, comercial, nómina y activos fijos) y 6 sub módulos contenidos por los módulos principales (Cuentas por pagar, cuentas por cobrar, inventarios, ventas, autoventas y contabilidad general), esta aplicación es accedida por usuarios de las 15 agencias (Bogotá, San Francisco, Guateque, Ubaque, Villeta, Suba, Soacha, Chinchiná, Armenia, Riosucio, Yumbo, Buenaventura, Popayán, Rio Negro, Copacabana) a través de VPN, SalesForce: Aplicación web y CRM (customer relationship management) en la que se hace seguimiento estricto y especifico a los clientes, en el que se almacena información de los contratos celebrados con los mismo, en el que se reportan casos y PQR (petición, queja o reclamo) por los agentes del call center, aplicación en la que se almacenan las hojas de vida de los activos tecnológicos de la compañía, las hojas de vida de los funcionarios, características relevantes de sus contratos y novedades de nómina. Saasmaint: Aplicación web en la que se hace estricto seguimiento a los vehículos de la compañía, en el que los funcionarios del área de mantenimiento vehicular ingresa información de los mantenimientos y compra de repuestos, incluyendo sus respectivas hojas de vida y documentos legales pertinentes.
Aplicaciones no core	Aplicaciones que soportan la operación del negocio que tienen criticidad baja, BIABLE: Aplicación que funciona como interfaz entre el Sistema UNO Ver. 8.5 Release 1502 y la base de datos MySQL, llevando la información de la base de datos en cobol a la bases de datos en MySQL, permitiendo realizar una extracción y análisis de información más rápida y eficiente. QLIKVIEW: Aplicación que funciona como sistema gestor de bases de datos SGBD, cumpliendo la función de integrar la información de las bases de datos del Sistema UNO Ver. 8.5, Salesforce y SaasMaint. ARCGIS: Aplicación con la que se hace seguimiento a la georreferenciación de clientes y puntos de venta, instalada en un servidor físico con sistema operativo Windows Server 2008 R2. B2B: Aplicación web que permite hacer seguimiento por GPS a los vehículos de la compañía.
Copias de seguridad	Copias de seguridad y backup de usuarios y servidores almacenados en 3 discos duros instalados en un servidor ubicado en el datacenter.
Matrices roles y privilegios	Matrices con la definición de los roles y privilegios de las aplicaciones y usuarios.

Cuadro 6. (Continuación)

Nombre Activo	Descripción
Equipos de cómputo de áreas administrativas y financieras	Equipos de cómputo de mesa y portátiles que almacenan y procesan información contable y financiera de la empresa utilizados en áreas como tesorería, contabilidad, cartera, facturación, georeferenciación, impuestos, recurso humano, Jurídica, calidad y operaciones; equipos ubicados en la sede administrativa principal en Bogotá, interconectados a través de la red local de la compañía y con los privilegios suficientes para acceder a las aplicaciones core, tales como, Sistema UNO Ver. 8.5, SalesForce, Saasmaint y aplicaciones no core.
Equipos de cómputo del área de tecnología	Equipos de cómputo utilizados para almacenar y procesar información del área de tecnología, tales como el laptop Toshiba Satélite L55 del coordinador de tecnología con los privilegios suficientes como para acceder y administrar las aplicaciones, servidores e infraestructura de la compañía; y el Dell Latitud del director de tecnología con los suficientes privilegios como para acceder y administrar las aplicaciones, servidores e infraestructura de la compañía.
Equipos de cómputo del área comercial	Equipos de cómputo utilizados para almacenar y procesar información del área comercial, como información de clientes y accesos al Sistema UNO Ver 8.5 Release 1502 como perfil de consulta y Salesforce con perfil únicamente de consulta.
Canales de internet y de comunicaciones	Canales de comunicación con usuarios y elementos externos, tales como la internet, la telefonía fija y telefonía móvil, ubicados en las 15 agencias de la compañía y tramitado con proveedores tales como, UNE, Telefónica, CLARO, MediaCommerce, EmCali, ALKnet, Inzanet y Avantel, los cuales han instalado canales de internet dedicados y en rehusó, con anchos de banda desde 1MB hasta 20 MB y canales de comunicación telefónica a través de SIP a nivel nacional y a nivel de móvil tramitando planes de minutos y datos definidos según el perfil del usuario.
Dispositivos de comunicación móvil	Equipos tecnológicos que permiten comunicación interna y externa, tales como, celulares, tabletas y teléfonos en general, en los que se tramita comunicación a través de llamadas directas, conferencias, chats a través de redes sociales como whatsap entre funcionarios de cargos auxiliares con las latas directivas.
Blade center	Dispositivo físico ubicado en el data center que cumple con la función de llevar a cabo un arreglo de servidores, ya que dicho dispositivo cuenta con el hardware necesario para almacenar varios sistema operativos en elementos conocidos como cuchillas, las cuales cuentan con hardware común de un equipo de cómputo, es decir, procesadores, memorias y discos duros, este equipo contiene los siguientes servidores: servidor de dominio, servidor de datos y servidor de aplicaciones no core.

Cuadro 6. (Continuación)

Nombre Activo	Descripción
Servidor CG1	Equipo de cómputo de gran desempeño o servidor marca Dell con referencia T610 el cual almacena un gestor de maquinar virtuales, en el que se cuenta con una máquina virtual con sistema operativo Linux Centos que contiene la aplicación core de la compañía (sistema UNO Ver 8.5 Release 1502)
CCTV	Dispositivos tecnológicos que componen el sistema del circuito cerrado de televisión CCTV, tales como 12 cámaras ubicadas estratégicamente en la sede administrativa de Bogotá, DVR con una capacidad de 3 TB, los cuales almacenan videos de seguridad de las 12 cámaras hasta un mes, para después empezar a sobrescribir.
Dispositivos de infraestructura de datos	Dispositivos tecnológicos que componen la infraestructura de datos y que permiten la comunicación a través de la red, tales como Switches y Routers marca 3COM, permitiendo la construcción de una red de área local con 4 subredes y configuraciones específicas de acceso.
Dispositivo de seguridad perimetral	Dispositivo de seguridad Dell Sonicwall NSA 2400 ubicado estratégicamente entre la red LAN y la WAN que gestiona la seguridad perimetral, dentro de este dispositivo se cuenta con antivirus, antispyware, anti spam, firewall, detección de intrusos, prevención de intrusos y control de navegación.
Dispositivos de impresión y digitalización	Dispositivos tecnológicos que permiten la impresión y digitalización de información ubicadas en las 15 agencias de la compañía.
Dispositivo de aire acondicionado	Dispositivo encargado de mantener una temperatura estable en el datacenter, por tal evita recalentamiento de dispositivos tecnológicos almacenados en operación.
Equipo de control de acceso	Elementos tecnológicos que componen el sistema de control de acceso, tales como tarjetas de proximidad, dispositivos lectores de tarjeta y equipo que almacena y procesa la aplicación
Fuente: Autores	

4.2 INVENTARIO DE ACTIVOS DE INFORMACIÓN

El inventario de activos es la base para la gestión de los mismos, ya que tiene que incluir toda la información necesaria para mantenerlos operativos e incluso poder recuperarse ante un desastre. Para facilitar el manejo y mantenimiento del inventario los activos se identifican los siguientes campos que permiten una mejor administración y gestión del activo de información:

- Código de Activo: Un código para ordenar y localizar los activos.

- Nombre de Activo: Nombre del activo de Información
- Descripción: Referencia que puede dar mayor conocimiento del activo
- Propietario: Cada uno de los activos que se identifiquen debe tener un responsable o propietario. Esta persona se hará cargo de mantener la seguridad del activo.
- Custodio Técnico: Delegado para implementar los controles de seguridad.

Todos los activos de información se deben identificar de manera adecuada, así como en el cuadro 7 Inventario de activos de Información.

Cuadro 7. Inventario de Activos de Información

Nombre del Activo de Información	**Descripción del Activo de Información**	**Tipo de Activo**
Manuales y procedimientos	Manuales y procedimientos del proceso de gestión de operaciones IT	Información Digital
Contratos	Contratos de servicios con proveedores	Información física
Bases de datos	CG1	Software
	SalesForce y SaasMaint	
	SQL Server (Biable)	
Actas	Actas de Entregas y Actas de Devolución	Información física
	Actas con proveedores	
Informes	Informes de Gestión	Activos físicos
	Informes de Operación	
Equipo de gestión de operaciones TI	Personal encargado de la gestión de Operaciones de IT (Dirección de Tecnología y Coordinación de Tecnología)	Tecnología

Cuadro 7. (Continuación)

Nombre del Activo de Información	Descripción del Activo de Información	Tipo de Activo
Data center	Granja de Servidores, Infraestructura de comunicaciones, CCTV, Control de acceso, Aire acondicionado	Tecnología
Aplicaciones core	Aplicaciones críticas para la operación del negocio, Sistema UNO CG1, SalesForce Saasmaint	Software
Aplicaciones no core	Aplicaciones que soportan la operación del negocio que tienen criticidad baja, BIABLE, QLIKVIEW, ARCGIS, y B2B	Software
Copias de seguridad	Copias de seguridad y backup de diferentes dispositivos	Activos físicos
Matrices roles y privilegios	matrices con la definición de los roles y privilegios de las aplicaciones	Información digital
Equipos de cómputo del áreas administrativas y financieras	Equipos de cómputo de mesa y portátiles que almacenan y procesan información contable y financiera de la empresa utilizados en áreas como tesorería, contabilidad, cartera, facturación, geo referenciación, impuestos, recurso humano, Jurídica, calidad y operaciones	Activos físicos
Equipos de cómputo del área de tecnología	Equipos de utilizados para almacenar y procesar información del área de tecnología	Activos físicos
Equipos de cómputo del área comercial	Equipos de cómputo utilizados para almacenar y procesar información del área comercial	Activos físicos
Canales de internet y de comunicaciones	Canales de comunicación con usuarios y elementos externos, tales como la internet, la telefonía fija y telefonía móvil	Activos físicos
Dispositivos de comunicación móvil	Equipos tecnológicos que permiten comunicación interna y externa, tales como, celulares, tabletas y teléfonos en general	Activos físicos
Blade center	Arreglo de servidores que contiene servidor de demonio, servidor de datos y servidor de aplicaciones no core	Activos físicos
Servidor CG1	Dispositivo tecnológico que contiene la aplicación core de la compañía (sistema UNO Ver 8.5)	Activos físicos
CCTV	Dispositivos tecnológicos que componen el sistema del CCTV, tales como cámaras, DVR y elementos de control	Activos físicos
Dispositivos de infraestructura de datos	Dispositivos tecnológicos que componen la infraestructura de datos y que permiten la comunicación a través de la red, tales como Switches y Routers.	Activos físicos

Cuadro 7. (Continuación)

Nombre del Activo de Información	Descripción del Activo de Información	Tipo de Activo
Dispositivo de seguridad perimetral (Dell Sonicwall NSA 2400)	Dispositivo de seguridad ubicado estratégicamente en la red LAN que gestiona la seguridad perimetral, dentro de este dispositivo se cuenta con antivirus, antispyware, anti spam, firewall, detección de intrusos y prevención de intrusos.	Activos físicos
Dispositivos de impresión y digitalización	Dispositivos tecnológicos que permiten la impresión y digitalización de información	Activos físicos
Dispositivo de aire acondicionado	Dispositivo encargado de mantener una temperatura estable en el datacenter, por tal evita recalentamiento de dispositivos tecnológicos almacenados en operación.	Activos físicos
Equipo de control de acceso	Elementos tecnológicos que componen el sistema de control de acceso, tales como tarjetas de proximidad, dispositivos lectores de tarjeta y equipo que almacena y procesa la aplicación	Activos físicos
Fuente: Autores		

4.3 VALORACIÓN DEL ACTIVO DE INFORMACIÓN

En el proceso de valoración de activos, se deben tener en cuenta todos los tipos de activos de información. Una vez identificados los activos, el siguiente paso a realizar es valorarlos, estimando el valor que tienen para la organización y cuál es su importancia para la misma. Para calcular este valor, se considera cual puede ser el daño o la afectación que puede suceder a un activo cuando se vea afectado en su disponibilidad, integridad y confidencialidad.

La valoración de los activos permite determinar los activos que son importantes para Combustibles Líquidos de Colombia S.A. ESP y para el proceso de tecnología, con los cuales se realizara el posterior análisis de riesgos.

Se debe valorar los activos de acuerdo con los atributos de confidencialidad, integridad y disponibilidad. Para realizar dicha valorización, se utiliza una escala cualitativa. En la tabla 2 se muestra cuáles son los criterios que se usaron para realizar la correcta valorización de estos activos:

Tabla 2. Referencia para valoración de activos de información

Atributo	Valor	Criterio	Descripción
Disponibilidad	1	Bajo	Debe estar disponible al menos el 10% del tiempo. No se requiere para soportar el proceso.
	2	Medio	El activo no está disponible y afecta parcialmente el proceso. Solo se requiere que esté disponible al menos el 50% del tiempo.
	3	Alto	La falta o no disponibilidad del activo de información impacta negativamente la prestación del servicio e impacta negativamente a la Organización. El activo debe estar siempre disponible.
Integridad	1	Bajo	No es relevante los errores que tenga o la información faltante
	2	Medio	Se afecta la Integridad del activo, sin embargo afecta parcialmente el proceso.
	3	Alto	Se afecta la Integridad del activo, y la pérdida de exactitud y estado completo del activo impacta negativamente la prestación del servicio.
Confidencialidad	1	Bajo	Se hace uso inadecuado de la información privilegiada a la cual se tiene acceso y los daños son muy bajos, el incidente no trasciende en la Organización.
	2	Medio	El conocimiento o divulgación no autorizada de la información impacta negativamente la misión y objetivos institucionales.
	3	Alto	El conocimiento o divulgación no autorizada de la información impacta negativamente la imagen y el personal de la Organización.

Fuente: Autores

Al valorar los activos de información, se obtienen las siguientes combinaciones de posibles valores que determinan la criticidad del activo (Ver tabla 3)

Tabla 3. Valores según nivel de criticidad

Valor	Criticidad
3	Bajo
4	Medio
5	Medio
6	Medio
7	Alto
8	Alto
9	Alto

Fuente: Autores

Al definir los posibles valores de los diferentes niveles de criticidad, el proceso de valoración de activos de información va ser más simple, tal y como se puede ver en el cuadro 8 Valoración de activos de información:

Cuadro 8. Valoración de activos de información

Registro de Activos			Nivel de protección Seguridad de la Información				
ID	**Nombre del Activo de Información**	**Descripción del Activo de Información**	**Tipo de Activo**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Nivel de criticidad**
TI1	Manuales y Procedimientos	Manuales y procedimientos del proceso de gestión de operaciones IT	Información Digital	Medio	Medio	Bajo	Medio
TI2	Contratos	Proveedores	Información física	Medio	Medio	Bajo	Medio
		Outsourcing					
TI3	Bases de Datos	CG1	Software	Alto	Alto	Alto	Alto
		SalesForce y SaasMaint					
		SQL Server (Biable)					
TI4	Actas	Actas de Entregas y Actas de Devolución	Información física	Medio	Medio	Medio	Medio
		Actas con proveedores					
TI5	Informes	Informes de Gestión	Activos físicos	Medio	Medio	Bajo	Medio
		Informes de Operación					

Cuadro 8. (Continuación)

Registro de Activos			Nivel de protección Seguridad de la Información				
ID	**Nombre del Activo de Información**	**Descripción del Activo de Información**	**Tipo de Activo**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Nivel de criticidad**
TI7	Data Center	Granja de Servidores, Infraestructura de comunicaciones, CCTV, Control de acceso, Aire acondicionado	Tecnología	Alto	Alto	Alto	Alto
TI8	Aplicaciones Core	Aplicaciones críticas, Sistema UNO CG1, SalesForce Saasmaint	Software	Alto	Alto	Alto	Alto
TI9	Aplicaciones no Core	Aplicaciones que soportan la operación del negocio que tienen criticidad baja, BIABLE, QLIKVIEW, ARCGIS, y B2B	Software	Medio	Medio	Bajo	Medio
TI10	Copias de seguridad	Copias de seguridad y backup.	Activos físicos	Alto	Medio	Medio	Alto
TI11	Matrices Roles y privilegios	matrices con la definición de los roles y privilegios de las aplicaciones	Información Digital	Alto	Medio	Medio	Alto
TI12	Equipos de cómputo del áreas administrativas y financieras	Equipos de cómputo de mesa y portátiles que almacenan y procesan información contable y financiera de la empresa utilizados en áreas como tesorería, contabilidad, cartera, facturación, geo referenciación, impuestos, recurso humano, Jurídica, calidad y operaciones	Activos físicos	Medio	Medio	Medio	Alto

Cuadro 8. (Continuación)

Registro de Activos			Nivel de protección Seguridad de la Información				
ID	**Nombre del Activo de Información**	**Descripción del Activo de Información**	**Tipo de Activo**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Nivel de criticidad**
TI13	Equipos de cómputo del área de tecnología	Equipos de cómputo utilizados para almacenar y procesar información del área de tecnología	Activos físicos	Alto	Medio	Medio	Alto
TI14	Equipos de cómputo del área comercial	Equipos de cómputo utilizados para almacenar y procesar información del área comercial	Activos físicos	Medio	Medio	Medio	Medio
TI15	Canales de internet y de comunicaciones	Canales de comunicación con usuarios y elementos externos, tales como la internet, la telefonía fija y telefonía móvil	Activos físicos	Medio	Alto	Alto	Alto
TI16	Dispositivos de comunicación móvil	Equipos tecnológicos que permiten comunicación interna y externa, tales como, celulares, tabletas y teléfonos en general	Activos físicos	Medio	Medio	Bajo	Medio

Cuadro 8. (Continuación)

Registro de Activos			Nivel de protección Seguridad de la Información				
ID	**Nombre del Activo de Información**	**Descripción del Activo de Información**	**Tipo de Activo**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Nivel de criticidad**
TI17	Blade Center	Arreglo de servidores que contiene servidor de demonio, servidor de datos y servidor de aplicaciones no core	Activos físicos	Alto	Alto	Alto	Alto
TI18	Servidor CG1	Dispositivo tecnológico que contiene la aplicación core de la compañía (sistema UNO Ver 8.5)	Activos físicos	Alto	Alto	Alto	Alto
TI19	CCTV	Dispositivos tecnológicos que componen el sistema del CCTV, tales como cámaras, DVR y elementos de control	Activos físicos	Alto	Alto	Alto	Alto
TI20	Dispositivos de infraestructura de datos	Dispositivos tecnológicos que componen la infraestructura de datos y que permiten la comunicación a través de la red, tales como Switches y Routers.	Activos físicos	Medio	Medio	Alto	Alto

Cuadro 8. (Continuación)

Registro de Activos			Nivel de protección Seguridad de la Información				
ID	**Nombre del Activo de Información**	**Descripción del Activo de Información**	**Tipo de Activo**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Nivel de criticidad**
TI21	Dispositivo de seguridad perimetral (Dell Sonicwall NSA 2400)	Dispositivo de seguridad ubicado estratégicamente en la red LAN que gestiona la seguridad perimetral, dentro de este dispositivo se cuenta con antivirus, antispyware, anti spam, firewall, detección de intrusos y prevención de intrusos.	Activos físicos	Alto	Alto	Alto	Alto
TI22	Dispositivos de impresión y digitalización	Dispositivos tecnológicos que permiten la impresión y digitalización de información	Activos físicos	Bajo	Medio	Medio	Medio
TI23	Dispositivo de aire acondicionado	Dispositivo encargado de mantener una temperatura estable en el datacenter, por tal evita recalentamiento de dispositivos tecnológicos almacenados en operación.	Activos físicos	Medio	Medio	Alto	Alto
TI24	Equipo de control de acceso	Elementos tecnológicos que componen el sistema de control de acceso, tales como tarjetas de proximidad, dispositivos lectores de tarjeta y equipo que almacena y procesa la aplicación	Activos físicos	Alto	Alto	Alto	Alto

Fuente: Autores

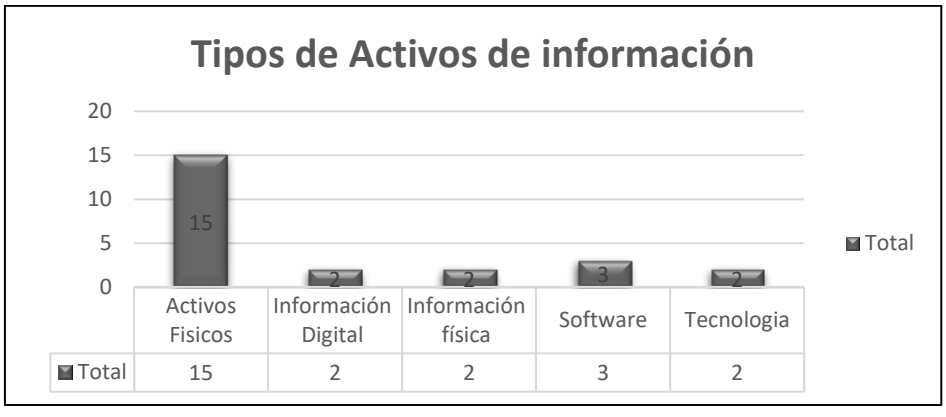
En la figura 14 se puede visualizar con claridad la distribución y clasificación de activos de acuerdo con el cuadro 8:

Figura 14. Clasificación de activos de información

Fuente: Autores

De la valoración de activos se puede inferir que de los 24 activos del proceso identificados, el 62% (15 activos) son clasificados como altos, lo cual quiere decir que son necesarios para el desarrollo de los procesos dado que la falta o no disponibilidad del activo de información impacta negativamente la prestación del servicio e impacta negativamente a la Organización; El activo debe estar siempre disponible. De igual forma, son esenciales para el proceso dado que se puede afectar su Integridad, y la pérdida de exactitud y estado completo del activo impacta negativamente la prestación del servicio. La información de los activos clasificados como altos, no debe ser divulgada sin autorización, dado que impacta negativamente la imagen y el personal de la Organización. (Ver figura 15)

Figura 15. Nivel de protección de seguridad de la información.



Fuente: Autores

De la clasificación también se puede conocer la distribución por tipos de activo, lo que permitirá enfocar el análisis de riesgos. La anterior figura, muestra los activos de información agrupados por el tipo de activo, en donde 15 de ellos corresponden a Activos físicos.

5. IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS

En este capítulo, se realiza la identificación y evaluación de los posibles riesgos, solo si se ha realizado un análisis de contexto y una identificación y clasificación de los activos de información de acuerdo con su confidencialidad, integridad y disponibilidad.

El resultado determina los controles y acciones necesarias que se deben implementar para proteger los activos de información y la continuidad del negocio, buscando que se establezca en Combustibles Líquidos de Colombia la gestión de los riesgos en cada uno de sus procesos.

De acuerdo con la norma ISO/IEC 27001:2013, la organización debe definir y aplicar un proceso de evaluación de riesgos de la seguridad de la información en donde:

"Se identifique los riesgos de la seguridad de la información:

- Aplicar el proceso de evaluación de riesgos de la seguridad de la información para identificar los riesgos asociados con la pérdida de confidencialidad, de integridad y de disponibilidad de información dentro del alcance del sistema de gestión de la seguridad de la información; e

- Identificar a los dueños de los riesgos[9]".

5.1 FACTORES DE RIESGO

Se entiende por factores de riesgo[10], las fuentes generadoras de eventos en las que se originan las pérdidas por riesgo. Son factores de riesgo el recurso humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos. Estos factores se deben clasificar en internos o externos.

- Recurso humano: Es el conjunto de personas vinculadas directa o indirectamente con la ejecución de los procesos de la entidad.

- Procesos**:** Es el conjunto interrelacionado de actividades para la transformación de elementos de entrada en productos o servicios, para satisfacer una necesidad.

---

[9] SUPERINTENDENCIA FINANCIERA. Norma ISO/IEC 27001:2013, 6.1.2 Evaluación de riesgos de la seguridad de la información. [En línea], [consultado el 3 de agosto de 2016]. Disponible en: https://www. superfinanciera.gov.co/SFCant/NormativaFinanciera/Archivos/ance048_06.rtf

- Tecnología**:** Es el conjunto de herramientas empleadas para soportar los procesos de la entidad. Incluye: hardware, software y comunicaciones.

- Infraestructura: Es el conjunto de elementos de apoyo para el funcionamiento de una organización. Entre otros se incluyen: edificios, espacios de trabajo, almacenamiento y transporte.

- Externos: Son situaciones asociadas a la fuerza de la naturaleza u ocasionados por terceros, que escapan en cuanto a su causa y origen al control de la entidad.

5.2 AMENAZAS Y VULNERABILIDADES DE LOS ACTIVOS DE INFORMACIÓN

Los activos están sometidos a muchos tipos de amenazas. Una amenaza tiene potencial de causar daño a un activo y por lo tanto a una organización. Este daño se puede presentar como un ataque sobre la información que es manejada por un sistema o servicio de TIC, sobre el sistema en si o sobre otros recursos como, por ejemplo, causando destrucción no autorizada, revelación, modificación, corrupción y no-disponibilidad o perdida. Una amenaza necesita aprovechar una vulnerabilidad existente en el activo para producirle daño. Las amenazas pueden tener origen ambiental o humano y, en el último caso, pueden ser accidentales o deliberadas[11].

Para este proceso, por cada activo de información se debe identificar las amenazas y vulnerabilidades a los cuales pueden estar expuestos, lo que determina las causas de riesgo presentes en los activos de información del proceso.

Lo más esencial es contar con un listado o catálogo de posibles amenazas a las cuales puedan estar expuestos los activos del proceso. El cuadro 9 es el catálogo de amenazas para el proceso de tecnología en Combustibles Líquidos de Colombia:

[11] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Norma Técnica Colombiana NTC 5411-1. Bogotá: ICONTEC, 2005

Cuadro 9. Catálogo de amenazas y vulnerabilidades

Amenaza	Vulnerabilidad
Daños a la Infraestructura	Controles de acceso al centro de datos inadecuados
	Perdida de suministro de energía
	Desastres naturales
	Ausencia de un sistema de prevención de Incendios
	Susceptibilidad a variaciones en la temperatura
	Ausencia de controles de acceso
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a variaciones en el voltaje
Manipulación de información	Error humano
	Roles y responsabilidades inadecuados
	Falta de capacitación
	Manipulación de datos e información
Acceso no autorizado	Abuso de derechos
	Software malicioso
	Abuso de derechos
	Falta de mecanismos de autenticación e identificación de usuarios
	Protección inadecuada
	Ausencia de controles de acceso
Manipulación de información	Error en el uso de software
Perdida de Información	Software malicioso
	Protección inadecuada
Continuidad del Negocio	Ausencia de planes de continuidad
Perdida de Información	Inadecuada clasificación de activos de información
	Falta de mecanismos de autenticación e identificación de usuarios
	Abuso de derechos
Daños a la Infraestructura	Degradación del sistema
Continuidad del Negocio	Perdida de suministro de energía
Perdida de Información	Software malicioso
	Inadecuada clasificación de activos de información.
	Protección inadecuada
Acceso no autorizado	Ausencia de procedimientos
	Falta de mecanismos de autenticación e identificación de usuarios
	Abuso de derechos
	Inadecuada clasificación de activos de información.
Fuente: Autores	

Una vulnerabilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas se conoce como vulnerabilidad. Las vulnerabilidades asociadas con los activos de información incluyen debilidades en el espacio físico, organización, procedimiento, personal, gestión, administración, hardware, software o información. Las amenazas pueden aprovechar vulnerabilidades para causar daño al sistema de TIC o a los objetivos del negocio. Una vulnerabilidad puede existir en ausencia de las amenazas correspondientes[12].

5.3 ANÁLISIS DE RIESGO

El análisis del riesgo implica ver y comprender el riesgo en un ambiente en donde no existen controles, con el propósito de identificar la probabilidad de ocurrencia de los riesgos y su impacto en caso de materializarse. Este análisis se realiza calculando la probabilidad e impacto de cada amenaza sobre cada activo de información.

La organización debe realizar un análisis de riesgo en donde:

"Se analice los riesgos de la seguridad de la información:

- Evaluando las potenciales consecuencias de si se materializaran los riesgos identificados;
- Evaluando la probabilidad de que ocurran los riesgos identificados;
- determinando los niveles de riesgo"[13].

5.4 NIVEL DE RIESGO

Se define diferentes niveles de riesgo, para permitir a la Organización, identificar cuales podrían generar un impacto significativo sobre la operación. En el cuadro 10 se describen los cinco niveles definidos para Combustibles Líquidos de Colombia:

[12] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Op. Cip. P. 90.
[13] ISO/IEC. Norma ISO/IEC 27001:2013, 6.1.2 Evaluación de riesgos de la seguridad de la información. Op. Cit. p. 25

Cuadro 10. Descripción niveles de riesgo

Nivel de riesgo	Descripción
Muy Alto	Riesgo muy alto significa que la materialización de una amenaza podría tener múltiples efectos adversos graves o catastróficos sobre el proceso y las operaciones de la organización, los activos de información, los individuos.
Alto	Riesgo alto significa que la materialización de una amenaza podría tener un efecto adverso grave o catastrófico sobre el proceso y las operaciones de la organización, los activos de información, los individuos.
Medio	Riesgo medio significa que la materialización de una amenaza podría tener un efecto adverso serio sobre el proceso y las operaciones de la organización, los activos de información, los individuos.
Bajo	Riesgo bajo significa que la materialización de una amenaza podría tener un efecto adverso limitado sobre el proceso y las operaciones de la organización, los activos de información, los individuos.
Muy Bajo	Riesgo muy bajo significa que la materialización de una amenaza podría tener un efecto adverso insignificante sobre el proceso y las operaciones de la organización, los activos de información, los individuos.
Fuente: Autores	

Durante la etapa de evaluación de riesgos se aceptan aquellos riesgos de nivel “Muy bajo”, “Bajo” y “Medio”, y por política no se deben aceptar los riesgos de nivel “Alto” y “Muy Alto” los cuales deben ser tratados.

5.4.1 Mapa de riesgos. Para identificarlos riesgos de acuerdo a su impacto y probabilidad, se utiliza un mapa de riesgo, el cual permite verlos de una forma gráfica; también se le llama mapa de calor, tal y como se muestra en el cuadro 11, en donde se utilizan dimensiones de 5x5:

Cuadro 11. Mapa de Calor

Muy Alto	PROBABILIDAD	**Medio**	**Alto**	**Alto**	**Muy Alto**	**Muy Alto**
Alto		**Medio**	**Medio**	**Alto**	**Alto**	**Muy Alto**
Medio		**Bajo**	**Medio**	**Medio**	**Alto**	**Alto**
Bajo		**Bajo**	**Bajo**	**Medio**	**Medio**	**Alto**
Muy Bajo		**Muy Bajo**	**Bajo**	**Bajo**	**Medio**	**Alto**
		IMPACTO				
		Muy Bajo	Bajo	Medio	Alto	Muy Alto
Fuente: Autores						

Al ubicar los riesgos en el mapa de riesgos, el dueño del proceso puede tomar decisiones respecto a la forma como debe abordarlos. El mapa es el resultado del análisis de riesgos que se hace en la matriz de riesgos.

5.5 EVALUACIÓN DE RIESGOS (VALORACIÓN)

La “valoración del riesgo”, se realiza estimando, cuál podría ser la probabilidad de ocurrencia del riesgo y el impacto que traería éste, en caso de materializarse.

Por probabilidad se entiende: la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de frecuencia, si se ha materializado (por ejemplo: Número de veces en un tiempo determinado), o de factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado. A continuación se describe cada nivel de probabilidad:

- Muy Alto, es casi seguro que la amenaza afecte la vulnerabilidad
- Alta, es probable que la amenaza afecte la vulnerabilidad
- Media, es posible que la amenaza afecte la vulnerabilidad
- Baja, es raro que la amenaza afecte la vulnerabilidad
- Muy Baja, es improbable que la amenaza afecte la vulnerabilidad

Por impacto se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo”[14]. A continuación se describe cada nivel de impacto, de acuerdo con la afectación que pueda haber sobre los procesos:

- Muy Alto, afecta por más de una semana los procesos y la operación
- Alta, afecta hasta en 72 horas los procesos y la operación
- Medio, afecta hasta en 24 horas los procesos y la operación
- Bajo, afecta hasta en 6 horas los procesos y la operación
- Muy Bajo, no tiene efecto en los procesos y la operación

La cuadro 12 determina el nivel de riesgo, de acuerdo con la calificación de la probabilidad y el impacto escogido para cada riesgo:

[14] MINISTERIO DE TECNOLOGÍA, INDUSTRIA Y COMERCIO. Definición de Probabilidad e Impacto, [En línea], [consultado el 3 de agosto de 2016]. Disponible en: http://www.mintic.gov.co/gestionti/615/articles-5482_Gestion_Riesgo.pdf

Cuadro 12. Probabilidad vs impacto

Probabilidad	Impacto	Nivel Riesgo
Muy bajo	Muy bajo	Muy Bajo
Muy bajo	Bajo	Bajo
Muy bajo	Media	Bajo
Muy bajo	Alto	Medio
Muy bajo	Muy Alto	Medio
Bajo	Muy bajo	Bajo
Bajo	Bajo	Bajo
Bajo	Media	Medio
Bajo	Alto	Medio
Bajo	Muy Alto	Moderado
Media	Muy bajo	Bajo
Media	Bajo	Medio
Media	Media	Medio
Media	Alto	Moderado
Media	Muy Alto	Moderado
Alto	Muy bajo	Medio
Alto	Bajo	Medio
Alto	Media	Moderado
Alto	Alto	Moderado
Alto	Muy Alto	Muy Alto
Muy Alto	Muy bajo	Medio
Muy Alto	Bajo	Moderado
Muy Alto	Media	Moderado
Muy Alto	Alto	Muy Alto
Muy Alto	Muy Alto	Muy Alto

Fuente: Autores

Las diferentes combinaciones permiten ubicar la valoración del activo en un mapa de calor, el cual es una herramienta que permite organizar la información sobre los riesgos del proceso y de la empresa, permitiendo visualizar su magnitud, con el fin de establecer las estrategias adecuadas para su manejo. Los mapas de riesgos pueden representarse con gráficos o datos. Los gráficos corresponden a la calificación de los riesgos con sus respectivas variables y a su evaluación de acuerdo con el método utilizado en cada empresa. Los datos pueden agruparse en tablas, con información referente a los riesgos; a su calificación, evaluación, controles y los demás datos que se requieran para contextualizar la situación de la empresa y sus procesos, con respecto a los riesgos que la pueden afectar y a las medidas de tratamiento implementadas[15].

[15] ESCUELA DE ADMINISTRACIÓN. Mapa de riesgos. [En línea], [consultado el 3 de agosto de 2016]. Disponible en: http://www.eafit.edu.co/escuelas/administracion/consultorio-contable/Documents / Nota %20de%20clase%2016%20Mapa%20de%20Riesgos.pdf

Luego de evaluar y definir la probabilidad y el impacto en el negocio que pueda ocasionar la materialización de los riesgos se obtiene el nivel del riesgo para cada activo de información, como se relaciona en la cuadro 13:

Cuadro 13. Matriz de riesgos

ID	Nombre del Activo de Información	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Nivel de Riesgo
TI6	Actas	Manipulación de información	Error Humano Roles y responsabilidades inadecuados Falta de Capacitación Manipulación de Datos e información	Bajo	Alto	Medio
TI25	Dispositivos de comunicación móvil	Daños a la Infraestructura	Controles de acceso al centro de datos inadecuados Perdida de suministro de energía Desastres naturales Ausencia de un sistema de prevención de Incendios Susceptibilidad a variaciones en la temperatura Ausencia de controles de acceso Sensibilidad a la radiación electromagnética Susceptibilidad a variaciones en el voltaje	Muy Alto	Muy bajo	Medio
TI26	Dispositivos de comunicación móvil	Acceso no autorizado	Abuso de derechos Software malicioso Abuso de derechos Falta de mecanismos de autenticación e identificación de usuarios Protección inadecuada Ausencia de controles de acceso	Muy Alto	Muy bajo	Medio
TI37	Dispositivos de impresión y digitalización	Daños a la Infraestructura	Controles de acceso al centro de datos inadecuados Perdida de suministro de energía Desastres naturales Ausencia de un sistema de prevención de Incendios Susceptibilidad a variaciones en la temperatura Ausencia de controles de acceso Susceptibilidad a variaciones en el voltaje	Media	Media	Medio

Cuadro 13. (Continuación)

ID	Nombre del Activo de Información	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Nivel de Riesgo
TI38	Dispositivos de impresión y digitalización	Acceso no autorizado	Abuso de derechos Software malicioso Abuso de derechos Falta de mecanismos de autenticación e identificación de usuarios Protección inadecuada Ausencia de controles de acceso	Media	Media	Medio
TI21	Equipos de cómputo del área comercial	Robo de equipos	Controles de acceso al centro de datos inadecuados Perdida de suministro de energía Desastres naturales Ausencia de un sistema de prevención de Incendios Susceptibilidad a variaciones en la temperatura Ausencia de controles de acceso Sensibilidad a la radiación electromagnética Susceptibilidad a variaciones en el voltaje	Bajo	Alto	Medio
TI22	Equipos de cómputo del área comercial	Acceso no autorizado	Abuso de derechos Software malicioso Abuso de derechos Falta de mecanismos de autenticación e identificación de usuarios Protección inadecuada Ausencia de controles de acceso	Bajo	Alto	Medio
TI17	Equipos de cómputo del áreas administrativas y financieras	Daños a la Infraestructura	Controles de acceso al centro de datos inadecuados Perdida de suministro de energía Desastres naturales Ausencia de un sistema de prevención de Incendios Susceptibilidad a variaciones en la temperatura Ausencia de controles de acceso Susceptibilidad a variaciones en el voltaje	Alto	Bajo	Medio

Cuadro 13. (Continuación)

ID	Nombre del Activo de Información	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Nivel de Riesgo
TI18	Equipos de cómputo del áreas administrativas y financieras	Acceso no autorizado	Abuso de derechos Software malicioso Abuso de derechos Falta de mecanismos de autenticación e identificación de usuarios Protección inadecuada Ausencia de controles de acceso	Alto	Bajo	Medio
TI7	Informes	Manipulación de información	Error Humano Roles y responsabilidades inadecuados Falta de Capacitación Manipulación de Datos e información	Bajo	Alto	Medio
TI16	Matrices Roles y privilegios	Acceso no autorizado	Abuso de derechos Software malicioso Abuso de derechos Falta de mecanismos de autenticación e identificación de usuarios Protección inadecuada Ausencia de controles de acceso	Alto	Bajo	Medio
TI12	Aplicaciones Core	Continuidad del Negocio	Perdida de suministro de energía	Alto	Alto	Moderado
TI13	Aplicaciones no Core	Continuidad del Negocio	Perdida de suministro de energía	Alto	Media	Moderado
TI4	Bases de Datos	Acceso no autorizado	Abuso de derechos Software malicioso Abuso de derechos Falta de mecanismos de autenticación e identificación de usuarios Protección inadecuada Ausencia de controles de acceso	Alto	Alto	Moderado
TI27	Blade Center	Daños a la Infraestructura	Controles de acceso al centro de datos inadecuados Perdida de suministro de energía Desastres naturales Ausencia de un sistema de prevención de Incendios Susceptibilidad a variaciones en la temperatura Ausencia de controles de acceso Sensibilidad a la radiación electromagnética Susceptibilidad a variaciones en el voltaje	Muy Alto	Media	Moderado

Cuadro 13. (Continuación)

ID	Nombre del Activo de Información	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Nivel de Riesgo
TI28	Blade Center	Continuidad del Negocio	Perdida de suministro de energía	Muy Alto	Media	Moderado
TI31	CCTV	Interrupción en los servicios	Controles de acceso al centro de datos inadecuados Perdida de suministro de energía Desastres naturales Ausencia de controles de acceso Susceptibilidad a variaciones en el voltaje	Muy Alto	Media	Moderado
TI32	CCTV	Acceso no autorizado	Abuso de derechos Software malicioso Abuso de derechos Falta de mecanismos de autenticación e identificación de usuarios Protección inadecuada Ausencia de controles de acceso	Muy Alto	Media	Moderado
TI2	Contratos	Manipulación de información	Error Humano Roles y responsabilidades inadecuados Falta de Capacitación Manipulación de Datos e información	Alto	Medio	Moderado
TI14	Copias de seguridad	Continuidad del Negocio	Perdida de suministro de energía	Alto	Alto	Moderado
TI15	Copias de seguridad	Perdida de Información	Software Malicioso Protección inadecuada	Alto	Alto	Moderado
TI10	Data Center	Perdida de Información	Software Malicioso Protección inadecuada	Media	Alto	Moderado
TI11	Data Center	Desastre Natural	Perdida de suministro de energía	Media	Alto	Moderado
TI9	Data Center	Ataques Externos / Internos	Controles de acceso al centro de datos inadecuados Perdida de suministro de energía Desastres naturales Ausencia de un sistema de prevención de Incendios Susceptibilidad a variaciones en la temperatura	Media	Muy Alto	Moderado
			Ausencia de controles de acceso Sensibilidad a la radiación electromagnética Susceptibilidad a variaciones en el voltaje			

Cuadro 13. (Continuación)

ID	Nombre del Activo de Información	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Nivel de Riesgo
TI39	Dispositivo de aire acondicionado	Interrupción en los servicios	Controles de acceso al centro de datos inadecuados Perdida de suministro de energía Desastres naturales Ausencia de un sistema de prevención de Incendios Susceptibilidad a variaciones en la temperatura Ausencia de controles de acceso Sensibilidad a la radiación electromagnética Susceptibilidad a variaciones en el voltaje	Alto	Media	Moderado
I40	Dispositivo de aire acondicionado	Acceso no autorizado	Abuso de derechos Software malicioso Abuso de derechos Falta de mecanismos de autenticación e identificación de usuarios Protección inadecuada Ausencia de controles de acceso	Alto	Media	Moderado
TI19	Equipos de cómputo del área de tecnología	Daños a la Infraestructura	Controles de acceso al centro de datos inadecuados Perdida de suministro de energía Desastres naturales Ausencia de un sistema de prevención de Incendios Susceptibilidad a variaciones en la temperatura Ausencia de controles de acceso Sensibilidad a la radiación electromagnética Susceptibilidad a variaciones en el voltaje	Muy Alto	Media	Moderado
TI20	Equipos de cómputo del área de tecnología	Acceso no autorizado	Abuso de derechos Software malicioso Abuso de derechos Falta de mecanismos de autenticación e identificación de usuarios Protección inadecuada Ausencia de controles de acceso	Media	Alto	Moderado

Cuadro 13. (Continuación)

ID	Nombre del Activo de Información	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Nivel de Riesgo
TI1	Manuales y Procedimientos	Perdida de Información	Software Malicioso Protección inadecuada	Alto	Medio	Moderado
TI29	Servidor CG1	Daños a la Infraestructura	Controles de acceso al centro de datos inadecuados Perdida de suministro de energía Desastres naturales Ausencia de un sistema de prevención de Incendios Susceptibilidad a variaciones en la temperatura Ausencia de controles de acceso Sensibilidad a la radiación electromagnética Susceptibilidad a variaciones en el voltaje	Alto	Alto	Moderado
TI30	Servidor CG1	Continuidad del Negocio	Perdida de suministro de energía	Alto	Alto	Moderado
TI3	Bases de Datos	Manipulación de información	Error Humano Roles y responsabilidades inadecuados Falta de Capacitación Manipulación de Datos e información	Muy Alto	Alto	Muy Alto
TI5	Bases de Datos	Perdida de Información	Software Malicioso Protección inadecuada	Muy Alto	Alto	Muy Alto
TI23	Canales de internet y de comunicaciones	Daños a la Infraestructura	Controles de acceso al centro de datos inadecuados Perdida de suministro de energía Desastres naturales Ausencia de un sistema de prevención de Incendios Susceptibilidad a variaciones en la temperatura Ausencia de controles de acceso Sensibilidad a la radiación electromagnética Susceptibilidad a variaciones en el voltaje	Muy Alto	Alto	Muy Alto
TI24	Canales de internet y de comunicaciones	Acceso no autorizado	Abuso de derechos Software malicioso Abuso de derechos Falta de mecanismos de autenticación e identificación de usuarios Protección inadecuada Ausencia de controles de acceso	Muy Alto	Alto	Muy Alto
TI35	Dispositivo de seguridad perimetral (Dell Sonicwall NSA 2400)	Daños a la Infraestructura	Controles de acceso al centro de datos inadecuados Perdida de suministro de energía Desastres naturales Ausencia de un sistema de	Muy Alto	Alto	Muy Alto

Cuadro 13. (Continuación)

ID	Nombre del Activo de Información	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Nivel de Riesgo
			Prevención de Incendios Susceptibilidad a variaciones en la temperatura. Ausencia de controles de acceso Sensibilidad a la radiación electromagnética. Susceptibilidad a variaciones en el voltaje.			
TI36	Dispositivo de seguridad perimetral (Dell Sonicwall NSA 2400)	Continuidad del Negocio	Perdida de suministro de energía	Muy Alto	Alto	Muy Alto
TI33	Dispositivos de infraestructura de datos	Daños a la Infraestructura	Controles de acceso al centro de datos inadecuados Perdida de suministro de energía Desastres naturales Ausencia de un sistema de prevención de Incendios Susceptibilidad a variaciones en la temperatura Ausencia de controles de acceso Sensibilidad a la radiación electromagnética Susceptibilidad a variaciones en el voltaje	Muy Alto	Alto	Muy Alto
TI34	Dispositivos de infraestructura de datos	Continuidad del Negocio	Perdida de suministro de energía	Muy Alto	Alto	Muy Alto
TI41	Equipo de control de acceso	Daños a la Infraestructura	Controles de acceso al centro de datos inadecuados Perdida de suministro de energía Desastres naturales Ausencia de un sistema de prevención de Incendios Susceptibilidad a variaciones en la temperatura Ausencia de controles de acceso Sensibilidad a la radiación electromagnética Susceptibilidad a variaciones en el voltaje	Muy Alto	Muy Alto	Muy Alto
TI42	Equipo de control de acceso	Continuidad del Negocio	Perdida de suministro de energía	Muy Alto	Muy Alto	Muy Alto
TI43	Equipo de control de acceso	Perdida de Información	Software Malicioso Protección inadecuada	Muy Alto	Muy Alto	Muy Alto
TI44	Equipo de control de acceso	Acceso no autorizado	Abuso de derechos Software malicioso Abuso de derechos Falta de mecanismos de autenticación e identificación de usuarios Protección inadecuada	Muy Alto	Muy Alto	Muy Alto

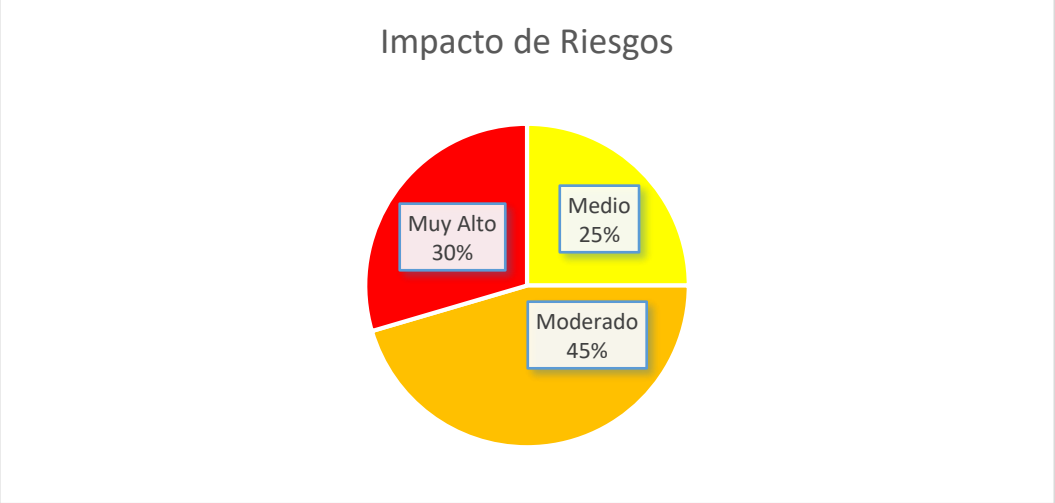
Cuadro 13. (Continuación)

ID	Nombre del Activo de Información	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Nivel de Riesgo
TI8	Equipo de gestión de Operaciones TI	Daños a la Infraestructura	Controles de acceso al centro de datos inadecuados Perdida de suministro de energía Desastres naturales Ausencia de un sistema de prevención de Incendios Susceptibilidad a variaciones en la temperatura Ausencia de controles de acceso Sensibilidad a la radiación electromagnética Susceptibilidad a variaciones en el voltaje	Muy Alto	Alto	Muy Alto

Fuente: Autores

Se identificaron 44 riesgos, los cuales de acuerdo a su nivel de riesgo, se distribuyen de la siguiente forma: 11(25%) clasificados como riesgo Medio, 20(45%) clasificados como riesgo Moderado y 13(30%) clasificados como riesgo Muy Alto. En la figura 16 se puede ver el peso de cada nivel de riesgo de acuerdo con la cantidad de riesgos identificados:

Figura 16. Distribución de riesgos por nivel de impacto



Fuente: Autores

Al ubicar los riesgos identificados en el mapa de riesgos, se obtiene un panorama de los riesgos, sobre los cuales se puede tomar decisiones. En el cuadro 14 o mapa de riesgos del proceso de tecnología en Combustibles Líquidos de Colombia, se ve la distribución de acuerdo a su impacto y probabilidad.

Cuadro 14. Mapa de riesgos del proceso de tecnología

Muy Alto	PROBABILIDAD	**TI25, TI26**		**TI19, TI27, TI28, TI31, TI32**	**TI3, TI5, TI8, TI23, TI24, TI33,TI34, TI35, TI36, TI41, TI42, TI43, TI44**	
Alto			**TI16, TI17, TI18**	**TI1, TI2, TI13, TI39, TI40**	**TI4, TI12, TI14, TI15, TI29, TI30**	
Medio				**TI37, TI38**	**TI10, TI11, TI20**	**TI9**
Bajo					**TI6, TI7, T21, T22**	
Muy Bajo						
		IMPACTO				
		Muy Bajo	Bajo	Medio	Alto	Muy Alto

Fuente: Autores

El plan de tratamiento debe aplicarse para cada uno de los riesgos. En este trabajo todos los riesgos deben tratarse, sin embargo se puede dar prioridad a los riesgos identificados en color ROJO, luego los identificados en el color naranja, luego los ubicados en el color amarillo y por último los ubicados en color verde.

6. PLAN DE TRATAMIENTO DE LOS RIESGOS

El plan de gestión de riesgos o plan de tratamiento de riesgos es la actividad en donde se define claramente cómo se va a actuar frente a cada riesgo identificado en cada activo de información. Para ello se identifica los recursos necesarios para implantar controles que mitiguen dichos riesgos. “Gestionar riesgos consiste principalmente en tomar decisiones con respecto a los distintos riesgos de acuerdo con la estrategia de la organización”[16].

De acuerdo con la norma ISO/IEC 27001, “aplicar un proceso de tratamiento de riesgos de la seguridad de la información permite:

- Seleccionar las opciones apropiadas de tratamiento de riesgos de la seguridad de la información, teniendo en cuenta los resultados de la evaluación de riesgos.

- Determinar todos los controles que sean necesarios para implementar las opciones escogidas para el tratamiento de riesgos de la seguridad de la información.

- Producir una declaración de aplicabilidad que contenga los controles necesarios y la justificación de las inclusiones, ya sea que se implementen o no, y la justificación para las exclusiones.

- Formular un plan de tratamiento de riesgos de la seguridad de la información.

- Obtener, de parte de los dueños de los riesgos, la aprobación del plan de tratamiento de riesgos de la seguridad de la información, y la aceptación de los riesgos residuales de la seguridad de la información.”

Con la gestión de los riesgos se busca adicionalmente seleccionar e implantar las medidas necesarias para reducir o controlar los riesgos identificados, de forma que los posibles daños que puedan causar se eliminen o se reduzcan lo más que se pueda. Un resultado del análisis de riesgos habrá sido el criterio para determinar cuáles van a ser los niveles de riesgo aceptables y en consecuencia, cuáles van a ser los niveles inaceptables y que por lo tanto son susceptibles de ser gestionados.

---

[16] ISOTOOLS COLOMBIA. El plan de gestión de riesgos según la norma ISO 27001- [En línea], [consultado el 3 de agosto de 2016]. Disponible en:https://www.isotools.org/2013/12/26/ el-plan-de-gestion-de-riesgos-segun-la-norma-iso-27001/

6.1 CRITERIOS PARA EL TRATAMIENTO DE RIESGOS

Para el tratamiento de riesgos se definen los siguientes tipos de criterios:

- Evitar. Establecer las medidas orientadas a prevenir su materialización.

- Reducir. Establecer medidas encaminadas a disminuir tanto la probabilidad mediante medidas de prevención, como el impacto mediante medidas de protección.

- Transferir. Reducir su efecto a través del traspaso del riesgo a otras organizaciones, como por ejemplo, asegurando el activo que tiene el riesgo o subcontratando el servicio.

- Asumir. Se asume el riesgo ya que está por debajo de un valor de riesgo aceptable, simplemente requiere que quede documentado y que se conoce y se acepta estos riesgos.

Los tipos de tratamientos se pueden ver reflejados en el mapa de riesgos, en donde los diferentes niveles de riesgo escogidos en el cuadro de 5 x 5 indicaran el tipo de tratamiento que se debe realizar. (Ver cuadro 15)

Cuadro 15. Criterios de aceptación

Muy Alto	----PROBABILIDAD--→	**Reducir**	**Transferir Reducir**	**Transferir Reducir**	**Evitar Transferir**	**Evitar Transferir**
Alto		**Reducir**	**Reducir**	**Transferir Reducir**	**Transferir Reducir**	**Evitar Transferir**
Medio		**Asumir**	**Reducir**	**Reducir**	**Transferir Reducir**	**Transferir Mitigar**
Bajo		**Asumir**	**Asumir**	**Reducir**	**Reducir**	**Transferir Reducir**
Muy Bajo		**Asumir**	**Asumir**	**Asumir**	**Reducir**	**Reducir**
		----------IMPACTO----------→				
		Muy Bajo	Bajo	Medio	**Alto**	Muy Alto

Fuente: Autores

El tratamiento de los riesgos, se puede resumir en la elaboración de 32 planes de acción, que buscan mitigar los riesgos identificados en el proceso de tecnología de Combustibles Líquidos de Colombia. (Ver Cuadro 16)

Cuadro 16. Tratamiento de los riesgos

Riesgo	Nombre del Activo de Información	Nivel de Riesgo	Plan de Tratamiento	Descripción del Plan de Acción
Acceso no autorizado	Bases de Datos Canales de internet y de comunicaciones CCTV Dispositivo de aire acondicionado Dispositivos de comunicación móvil Dispositivos de impresión y digitalización Equipo de control de acceso Equipos de cómputo del área comercial Equipos de cómputo del área de tecnología Equipos de cómputo del áreas administrativas y financieras Matrices Roles y privilegios	Moderado	Transferir Reducir	* Realizar pruebas de hacking Ético para identificar vulnerabilidades y definir un nivel de protección de la infraestructura de TI. * Realizar campañas de Seguridad a los usuarios de la red. * Revisar periódicamente los roles y usuarios, de las diferentes aplicaciones. * Revisar de inmediato lo roles y perfiles * Implementar la política del menor privilegio sobre los diferentes sistemas * Implementar doble factor de autenticación * Fortalecer el control de acceso * Adquirir una solución para el monitoreo de Logs y correlación de eventos. * Establecer un procedimiento para la asignación de roles y privilegios. * Implementar un procedimiento de monitoreo del antivirus. * Implementar políticas de control de acceso
	Canales de internet y de comunicaciones	Muy Alto	Evitar Transferir	* Realización y ejecución de las pruebas de continuidad. * Revisión de los privilegios de administradores. * Implementar la política de control de acceso. * Realización y ejecución de las pruebas de continuidad. * Restringir el acceso a los equipos de comunicaciones, implementando controles de acceso adicionales. * Fortalecer los controles de acceso * Revisión periódica de las UPS y certificación de los puntos de red. * Implementación de control de acceso a la red en los switches por puerto y dirección MAC de los equipos.
Ataques Externos / Internos	Data Center	Moderado	Transferir Reducir	* Revisión del control de acceso al Datacenter * Realizar pruebas de continuidad y recuperación de desastres. * Implementar bitácora para el acceso al Datacenter. * Implementar sistema de CCTV en el Datacenter.
Continuidad del Negocio	Aplicaciones Core Aplicaciones no Core Blade Center Copias de seguridad Dispositivo de seguridad perimetral (Dell Sonicwall NSA 2400)	Moderado	Transferir Reducir	Realización y ejecución de las pruebas de continuidad.

Cuadro 16. (Continuación)

Riesgo	Nombre del Activo de Información	Nivel de Riesgo	Plan de Tratamiento	Descripción del Plan de Acción
Continuidad del Negocio	Dispositivos de infraestructura de datos Equipo de control de acceso Servidor CG1	Moderado	Transferir Reducir	Realización y ejecución de las pruebas de continuidad.
Daños a la Infraestructura	Blade Center Canales de internet y de comunicaciones Dispositivo de seguridad perimetral (Dell Sonicwall NSA 2400) Dispositivos de comunicación móvil Dispositivos de impresión y digitalización Dispositivos de infraestructura de datos Equipo de control de acceso Equipo de gestión de Operaciones TI Equipos de cómputo del área de tecnología Equipos de cómputo del áreas administrativas y financieras Servidor CG1	Muy Alto	Evitar Transferir	* Realización y ejecución de las pruebas de continuidad. * Revisión de los privilegios de administradores. * Implementar la política de control de acceso. * Realización y ejecución de las pruebas de continuidad. * Restringir el acceso a los equipos de comunicaciones, implementando controles de acceso adicionales. * Fortalecer los controles de acceso * Revisión periódica de las UPS y certificación de los puntos de red. * Implementación de control de acceso a la red en los switches por puerto y dirección MAC de los equipos.
Desastre Natural	Data Center	Moderado	Transferir Reducir	Realización y ejecución de las pruebas de continuidad.
Interrupción en los servicios	CCTV Dispositivo de aire acondicionado	Moderado	Transferir Reducir	* Realización y ejecución de las pruebas de continuidad. * Revisión de los privilegios de administradores. * Implementar la política de control de acceso.
Manipulación de información	Actas Informes	Medio	Reducir	* Implementar controles de versiones. * Implementar herramientas de prevención de fuga de información.
Manipulación de información	Bases de Datos	Muy Alto	Evitar Transferir	* Replicar la información de las bases de datos, al datacenter alterno. * Limitar el acceso a los sistemas con credenciales de administrador. * Custodiar las claves de administrador y DBA, y solo usarla en los casos en los que se requiera * Solo los cambios autorizados por el comité de cambios se deben realizar en ambiente productivo.
	Contratos	Moderado	Transferir Reducir	* Implementar un procedimiento de monitoreo del antivirus. * Implementar políticas de control de acceso

Cuadro 16. (Continuación)

Riesgo	Nombre del Activo de Información	Nivel de Riesgo	Plan de Tratamiento	Descripción del Plan de Acción
Perdida de Información	Bases de Datos Equipo de control de acceso	Muy Alto	Evitar Transferir	* Realizar análisis de vulnerabilidades y ethical hacking.
	Data Center Manuales y Procedimientos Copias de seguridad	Moderado	Transferir Reducir	* Restringir los puertos USB y unidades de CD/DVD en los servidores. * Restringir el acceso a Internet en el datacenter. * Implementar un procedimiento de monitoreo del antivirus. * Implementar políticas de control de acceso * Realizar pruebas de restauración de las copias de seguridad. * Actualizar la política de backup * Llevar las copias de seguridad a un lugar fuera de las instalaciones de Combustibles Líquidos de Colombia.
Robo de equipos	Equipos de cómputo del área comercial	Medio	Reducir	* Realización y ejecución de las pruebas de continuidad. * Implementar un procedimiento de monitoreo * Realizar análisis de ingeniería social

Fuente: Autores

Cada plane de acción está relacionado con la política de control de acceso, y con el monitoreo que se debe implementar en la infraestructura de utilizada por el proceso de tecnología en Combustibles Líquidos de Colombia. En el cuadro 17 se resumen los planes definidos, en donde se describen los planes de acción precisados para Combustibles Líquidos de Colombia SA ESP.

Cuadro 147. Planes de acción

Planes de acción
* Adquirir una solución para el monitoreo de Logs y correlación de eventos.
* Custodiar las claves de administrador y DBA, y solo usarla en los casos en los que se requiera.
* Actualizar la política de backup
* Establecer un procedimiento para la asignación de roles y privilegios.
* Fortalecer los controles de acceso
* Implementación de control de acceso a la red en los switches por puerto y dirección MAC de los equipos.
* Implementar bitácora para el acceso al Datacenter.
* Implementar controles de versiones.
* Implementar doble factor de autenticación
* Implementar herramientas de prevención de fuga de información.
* Implementar la política de control de acceso.
* Implementar la política del menor privilegio sobre los diferentes sistemas
* Implementar sistema de CCTV en el datacenter.
* Implementar un procedimiento de monitoreo
* Limitar el acceso a los sistemas con credenciales de administrador.
* Llevar las copias de seguridad a un lugar fuera de las instalaciones de Combustibles Líquidos de Colombia.
* Realización y ejecución de las pruebas de continuidad.
* Realizar análisis de vulnerabilidades y ethical hacking.
* Realizar campañas de Seguridad a los usuarios de la red.
* Realizar pruebas de continuidad y recuperación de desastres.
* Realizar pruebas de hacking Ético para identificar vulnerabilidades y definir un nivel de protección de la infraestructura de TI.
* Realizar pruebas de restauración de las copias de seguridad.
* Replicar la información de las bases de datos, al datacenter alterno.
* Restringir el acceso a Internet en el datacenter.
* Restringir los puertos USB y unidades de CD/DVD en los servidores.
* Revisar de inmediato lo roles y perfiles
* Revisar periódicamente los roles y usuarios, de las diferentes aplicaciones.
* Revisión de los privilegios de administradores.
* Revisión del control de acceso al Datacenter
* Revisión periódica de las UPS y certificación de los puntos de red.
* Solo los cambios autorizados por el comité de cambios se deben realizar en ambiente productivo.
Fuente: Autores

Para terminar el plan de tratamiento, se seleccionaron los controles que mitigan los riesgos identificados, los cuales son los que se detallan en el anexo 1 de la norma ISO/IEC 27001 apartados 5 a 18; El cuadro 18 es una lista bastante completa de objetivos de control y controles comúnmente relevantes para las organizaciones en general. Se definió los controles asociados a las políticas de seguridad que responden a los riesgos identificados y a los planes de acción requeridos. Todos estos controles o políticas contribuyen a la mitigación de todos los riesgos identificados. En el cuadro 18 se relacionan los controles y políticas de seguridad que se deben implementar en Combustibles Líquidos de Colombia:

Cuadro 18. Controles específicos de la seguridad de la información

ISO 27001:2005 controles - anexo a		Riesgo	Descripción
Sección	**Objetivo de control / control**		
5. Políticas de la seguridad de la información			
5.1	**Orientación de la dirección para la gestión de la seguridad de la información.** **Objetivo:** Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.		
5.1.1	Políticas para la seguridad de la información.	Todos	La alta gerencia de Combustibles Líquidos de Colombia debe aprobar un documento de política de seguridad de la información, publicarlo y comunicarlo a todos los empleados y partes interesadas, adicionalmente la debe revisar por lo menos una vez al año o antes si se producen cambios en el proceso o en la organización, cambios significativos, para asegurar su idoneidad, adecuación y eficacia continuas.
5.1.2	Revisión de las políticas para seguridad de la información.		
6. Organización de la seguridad de la información			
6.1	**Organización Interna.** **Objetivo:** Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.		
6.1.1	Seguridad de la información, Roles y responsabilidades	Todos	* Se deben definir y asignar todas las responsabilidades de la seguridad de la información. * Las tareas y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
6.1.2	Separación de Deberes		
8. Gestión de activos			
8.1	**Responsabilidad por los activos.** **Objetivo:** Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.		
8.1.1	Inventario de activos.	Todos	* Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, * Identificar un propietario
8.1.2	Propiedad de los activos.		
8.1.3	Uso aceptable de los activos.		

Cuadro 18. (Continuación)

ISO 27001:2005 Controles - Anexo A		Riesgo	Descripción
Sección	**Objetivo de control / control**		
8.2	**Clasificación de la Información.** **Objetivo:** Asegurar que la organización recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.		
8.2.1	Clasificación de la Información.	TI1, TI2. TI6 TI7, TI14	* La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. * Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
8.2.2	Etiquetado de la información.		
8.2.3	Manejo de activos.		
9. Control de acceso			
9.1	**Requisitos del negocio para el control de acceso.** **Objetivo:** Limitar el acceso a información y a instalaciones de procesamiento de información.		
9.1.1	Política de control de acceso.	TI4, TI16, TI18 TI20, TI22, TI24 TI26, TI32, TI38 TI40, TI44	* Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
9.1.2	Acceso a redes y a servicios en red.		
9.2	**Gestión de Acceso de Usuarios.** **Objetivo:** Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.		
9.2.1	Registro y cancelación del registro de usuarios.	TI4, TI8, TI10 TI12, TI13, TI13 TI18, TI20, TI22 TI24, TI26, TI27 TI29, TI32, TI33 TI35, TI38, TI40 TI41, TI44	* Se debe implementar un proceso formal de registro y de cancelación del registro, para posibilitar la asignación de los derechos de acceso * Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado. * Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
9.2.2	Suministro de acceso de usuarios.		
9.2.3	Gestión de derechos de acceso privilegiado.		
9.2.4	Gestión de información de autenticación secreta de usuarios.		
9.2.5	Revisión de los derechos de acceso de usuarios.		
9.2.6	Cancelación o ajuste de los derechos de acceso.		
9.4	**Control de Acceso a Sistemas y Aplicaciones.** **Objetivo:** Prevenir el uso no autorizado de sistemas y de aplicaciones.		
9.4.1	Restricción del acceso a la información.	TI4, TI8, TI10 TI12, TI13, TI13 TI18, TI20, TI22 TI24, TI26, TI27 TI29, TI32, TI33 TI35, TI38, TI40 TI41, TI44	* El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso. * Se debe restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.
9.4.2	Procedimiento de conexión segura.		
9.4.3	Sistema de gestión de contraseñas.		
9.4.4	Uso de programas utilitarios privilegiados.		
9.4.5	Control de acceso al código fuente de los programas.		

Cuadro 18. (Continuación)

ISO 27001:2005 Controles - Anexo A		Riesgo	Descripción
Sección	**Objetivo de control / control**		
11. Seguridad física y ambiental			
11.1	**Áreas Seguras.** **Objetivo:** Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.		
11.1.3	Seguridad de oficinas, salones e instalaciones.	T19	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información * Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
11.1.4	Protección contra amenazas externas y ambientales.		
11.1.5	Trabajo en áreas seguras.		
11.1.6	Áreas de despacho y carga.		
11.2	**Seguridad de los Equipos.** **Objetivo:** Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.		
11.2.1	Ubicación y protección de los equipos.	TI8 TI17 TI19 TI21 TI41	* Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, y las posibilidades de acceso no autorizado * Los equipos se deben proteger de fallas de potencia y otras interrupciones causadas por fallas en los servicios públicos de soporte. * Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información
11.2.2	Servicios de públicos de soporte.		
11.2.3	Seguridad del cableado.		
11.2.4	Mantenimiento de los equipos.		
11.2.5	Retiro de activos.		
11.2.6	Seguridad de equipos y activos fuera de las instalaciones (predio).		
11.2.7	Disposición segura o reutilización de equipos.		
11.2.8	Equipo de usuario desatendido.		
11.2.9	Política de escritorio limpio y pantalla limpia.		
12.1	**Procedimientos Operacionales**		
12.1.1	Gestión de Cambios	TI8, TI17, TI19 TI21, TI41	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información
12.1.2	Gestión de Capacidad	TI8, TI17, TI19 TI21, TI41	Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema
12.4.1	Registro de Eventos	TI8, TI17, TI19 TI21, TI41	Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

Cuadro 18. (Continuación)

ISO 27001:2005 Controles - Anexo A		Riesgo	Descripción
Sección	**Objetivo de control / control**		
12.6	**Gestión de la Vulnerabilidad Técnica.** **Objetivo:** Prevenir el aprovechamiento de las vulnerabilidades técnicas.		
12.6.1	Control de las vulnerabilidades técnicas.	TI1, TI4, TI5 TI10, TI15, TI16 TI18, TI20, TI22 TI24, TI26,TI32 TI38, TI40, TI43 TI44	* Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
12.6.2	Restricciones sobre la instalación de software.		
12.4.1	Registro de Eventos		
12.5.1	Instalación de software en sistemas operativos		Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos
13.1	Gestión de la seguridad de redes		
13.1.1	Controles de redes	TI25, TI33, TI35 ,TI41	* Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones
13.1.2	Seguridad de los servicios de red		
13.1.3	Separación en las redes		
16. Gestión de incidentes de seguridad de la información			
16.1	**Gestión de incidentes y mejoras en la seguridad de la información.** **Objetivo:** Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.		
16.1.1	Responsabilidades y procedimientos.	Todos	* Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. * Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información. * Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
16.1.2	Informe de eventos de seguridad de la información.		
16.1.3	Informe de debilidades de seguridad de la información.		
16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.		
16.1.5	Respuesta a incidentes de seguridad de la información.		

Cuadro 18. (Continuación)

ISO 27001:2005 Controles - Anexo A		Riesgo	Descripción
Sección	**Objetivo de control / control**		
17. Aspectos de seguridad de la información de la gestión de continuidad de negocio.			
17.1	**Continuidad de seguridad de la información.** **Objetivo:** La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.		
17.1.1	Planificación de la continuidad de la seguridad de la información.	TI11, TI12, TI13, TI14 TI28, TI30, TI34, TI36 TI42	* La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre. * La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
17.1.2	Implementación de la continuidad de la seguridad de la información.		
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.		
17.2	**Redundancias** **Objetivo:** Asegurarse de la disponibilidad de instalaciones de procesamiento de información.		
17.2.1	Disponibilidad de instalaciones de procesamiento de información.	TI9	* Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad

Fuente: Autores

6.2 DECLARACIÓN DE APLICABILIDAD

El resultado de la identificación de los controles seleccionados para el tratamiento de los riesgos, para el proceso de tecnología en Combustibles Líquidos de Colombia, es la declaración de aplicabilidad, la cual es uno de los elementos principales de un sistema de gestión de seguridad de la información. En la declaración de aplicabilidad se relaciona los controles que se aplican en el sistema de gestión.

El anexo A de la norma ISO/IEC 27001:2013, propone 111 controles, de los cuales se deben seleccionar aquellos que se quieren implantar para el dar respuesta a los riesgos identificados. El resultado de la elección de los controles forma parte del plan de tratamiento de riesgos, de modo que éste tiene como salida la declaración de aplicabilidad.

Cada control que no es implementado de los 111 propuestos por la norma, se debe justificar por qué no se va a utilizar. De igual forma, pueden existir controles adicionales a los descritos, con el objetivo de incrementar los niveles de seguridad de la información en el proceso y en la organización. El cuadro 19 corresponde a la declaración de aplicabilidad para Combustibles Líquidos de Colombia:

Cuadro 19. Declaración de aplicabilidad

ISO 27001:2005 Controles – Anexo A			Aplica (Si/No)	Justificación
Dominio	**Sección**	**Control**		
5. Políticas de la seguridad de la información	**5. Políticas de la seguridad de la información**			
	5.1	**Orientación de la dirección para la gestión de la seguridad de la información.** **Objetivo:** Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.		
	5.1.1	Políticas para la seguridad de la información.	SI	Se adopta este control, se debe definir un conjunto de políticas para la seguridad de la Información, aprobadas por la dirección, publicadas y comunicadas a los empleados y partes externas.
	5.1.2	Revisión de las políticas para seguridad de la información.	SI	Se adopta este control, puesto que las políticas se deben revisar a intervalos planificados, o sí ocurren cambios significativos para asegurar su conveniencia, adecuación y eficacias continuas.
6. Organización de la Seguridad de la Información	**6. Organización de la seguridad de la información**			
	6.1	**Organización Interna.** **Objetivo:** Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.		
	6.1.1	Seguridad de la información, Roles y responsabilidades	SI	La organización a través de la política de seguridad de la información debe establecer el compromiso, organización y asignación de responsabilidades para su cumplimiento. Se adopta este control, puesto que se deben mantener contactos apropiados con los grupos de interés especial, o foros, o asociaciones profesionales especializadas en seguridad.
	6.1.2	Separación de Deberes	SI	
	6.1.3	Contacto con las autoridades.	SI	
	6.1.4	Contacto con grupos de interés especial.	SI	
	6.1.5	Seguridad de la Información en gestión de proyectos	SI	
	6.2	**Dispositivos móviles y teletrabajo.** **Objetivo:** Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.		
	6.2.1	Política para dispositivos móviles	SI	La organización restringe la conexión a las redes inalámbricas de internet por parte de los dispositivos móviles y equipos de terceros.
	6.2.2	Teletrabajo	NO	Combustibles líquidos no cuenta con Teletrabajo, el cual es una forma de organización laboral, que consiste en el desempeño de actividades utilizando como soporte las tecnologías de la información y las comunicaciones – TIC para el contacto entre el trabajador y la empresa. Por lo tanto considera que no se aplica el control.

Cuadro 19. (Continuación)

ISO 27001:2005 Controles – Anexo A			Aplica (Si/No)	JUSTIFICACIÓN
Dominio	**Sección**	**Control**		
7. Seguridad de los Recursos Humanos	**7. Seguridad de los recursos humanos**			
	7.1	**Antes de asumir el empleo.** **Objetivo:** Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.		
	7.1.1	Selección.	SI	Se adopta este control, puesto que la verificación de antecedentes de todos los aspirantes a un empleo se deben llevar a cabo y deben ser proporcionales a los requisitos del negocio, a la clasificación de la información a la cual va a tener acceso, y a los riesgos identificados.
	7.1.2	Términos y condiciones del empleo.	SI	
	7.2	**Durante la ejecución del empleo.** **Objetivo:** Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.		
	7.2.1	Responsabilidades de la dirección.	SI	Se adopta el control, con el cual se quiere formar consciencia de los riesgos, responsabilidades y deberes con respecto a seguridad de la información; igualmente es necesario capacitar al personal en temas de seguridad de la información; También se hace preciso establecer un proceso disciplinario que permita a la organización saber cómo actuar en caso de que los colaboradores cometan alguna violación de la seguridad
	7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	SI	
	7.2.3	Proceso disciplinario.	SI	
	7.3	**Terminación y cambio de empleo.** **Objetivo:** Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.		
	7.3.1	Terminación o cambio de responsabilidades de empleo.	SI	Se adopta este control, puesto que las responsabilidades y los deberes de Seguridad de la Información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.

Cuadro 19. (Continuación)

ISO 27001:2005 Controles – Anexo A			Aplica (SI/NO)	Justificación
Dominio	**Sección**	**Control**		
8. Gestión de Activos	**8. Gestión de activos**			
	8.1	**Responsabilidad por los activos.** **Objetivo:** Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.		
	8.1.1	Inventario de activos.	SI	Dentro del proceso de implementación y mantenimiento del SGSI se debe realizar un inventario de todos los activos de información, en tal sentido es importante identificar los propietarios de estos, realizar un inventario, y también garantizar el uso adecuado de los mismos a través de políticas documentadas e implementadas.
	8.1.2	Propiedad de los activos.	SI	
	8.1.3	Uso aceptable de los activos.	SI	
	8.1.4	Devolución de activos.	SI	
	8.2	**Clasificación de la Información.** **Objetivo:** Asegurar que la organización recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.		
	8.2.1	Clasificación de la Información.	SI	Se deben implementar controles y procedimientos que permitan dar a la información de la empresa el nivel adecuado de protección, etiquetado y manejo con base en la clasificación de información que se utilice, tomando en cuenta su valor, los requisitos legales, la sensibilidad y la importancia para la organización.
	8.2.2	Etiquetado de la información.	SI	
	8.2.3	Manejo de activos.	SI	
	8.3	**Manejo de medios de soporte.** **Objetivo:** Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte.		
	8.3.1	Gestión de medios de soporte removibles.	SI	Se adopta este control, puesto que se debe establecer controles para asegurar que se eviten eventos como divulgación, modificación, retiro o destrucción de información no autorizada.
	8.3.2	Disposición de los medios de soporte.	SI	
	8.3.3	Transferencia de medios de soporte físicos.	SI	

Cuadro 19. (Continuación)

ISO 27001:2005 Controles – Anexo A			Aplica (SI/NO)	Justificación
Dominio	**Sección**	**Control**		
9. Control de Acceso	**9. Control de acceso**			
	9.1	**Requisitos del negocio para el control de acceso.** **Objetivo:** Limitar el acceso a información y a instalaciones de procesamiento de información.		
	9.1.1	Política de control de acceso.	SI	Se adopta este control, puesto que se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información. Es importante establecer controles de seguridad que permitan asegurar que los propietarios de activos de información controlan el acceso a la información.
	9.1.2	Acceso a redes y a servicios en red.	SI	
	9.2	**Gestión de Acceso de Usuarios.** **Objetivo:** Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.		
	9.2.1	Registro y cancelación del registro de usuarios.	SI	Se adopta este control, puesto que es importante establecer controles de seguridad que aseguren el acceso de usuarios autorizados así como permitan evitar el acceso de usuarios no autorizados a información.
	9.2.2	Suministro de acceso de usuarios.	SI	
	9.2.3	Gestión de derechos de acceso privilegiado.	SI	
	9.2.4	Gestión de información de autenticación secreta de usuarios.	SI	
	9.2.5	Revisión de los derechos de acceso de usuarios.	SI	
	9.2.6	Cancelación o ajuste de los derechos de acceso.	SI	
	9.3	**Responsabilidades de los Usuarios.** **Objetivo:** Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.		
	9.3.1	Uso de información de autenticación secreta.	SI	Se adopta este control, puesto que se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.

Cuadro 19. (Continuación)

ISO 27001:2005 Controles – Anexo A			Aplica (SI/NO)	Justificación
Dominio	**Sección**	**Control**		
9. Control de Acceso	9.4	**Control de Acceso a Sistemas y Aplicaciones.** **Objetivo:** Prevenir el uso no autorizado de sistemas y de aplicaciones.		
	9.4.1	Restricción del acceso a la información.	SI	Se adopta este control, puesto que el acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
	9.4.2	Procedimiento de conexión segura.	SI	
	9.4.3	Sistema de gestión de contraseñas.	SI	
	9.4.4	Uso de programas utilitarios privilegiados.	SI	
	9.4.5	Control de acceso al código fuente de los programas.	SI	
10. Criptografía	**10. Criptografía**			
	10.1	**Controles Criptográficos.** **Objetivo:** Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de información.		
	10.1.1	Política sobre el uso de controles criptográficos.	SI	Se adopta el control dado que se requiere definir para cada sistema de información en donde se tenga información crítica o confidencial, controles criptográficos con el objetivo de garantizar la confidencialidad e integridad de la información.
	10.1.2	Gestión de claves.	SI	
11. Seguridad física y Ambiental	**11. Seguridad física y ambiental**			
	11.1	**Áreas Seguras.** **Objetivo:** Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.		
	11.1.1	Perímetro de seguridad física.	SI	Se adopta este control, puesto que es importante establecer los controles de seguridad para evitar el acceso físico no autorizado, el daño a la infraestructura y activos de información de la compañía.
	11.1.2	Controles físicos de entrada.	SI	
	11.1.3	Seguridad de oficinas, salones e instalaciones.	SI	
	11.1.4	Protección contra amenazas externas y ambientales.	SI	
	11.1.5	Trabajo en áreas seguras.	SI	
	11.1.6	Áreas de despacho y carga.	SI	Se adopta este control, puesto que en Combustibles Líquidos de Colombia se tienen un área de carga o despacho, por tal razón es necesario establecer controles

Cuadro 19. (Continuación)

ISO 27001:2005 Controles – Anexo A			Aplica (SI/NO)	Justificación
Dominio	**Sección**	**Control**		
11. Seguridad física y Ambiental	11.2	**Seguridad de los Equipos.** **Objetivo:** Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.		
	11.2.1	Ubicación y protección de los equipos.	SI	Se adopta este control, puesto que en Combustibles Líquidos se usan equipos tales como servidores, computadores de escritorio, portátiles, impresoras, fotocopiadoras, faxes, escáneres, entre otros, en los cuales se procesa la información de los diferentes sistemas de información. Por tal razón es necesario establecer controles que permitan evitar la ocurrencia de eventos como pérdida, daño, robo o interrupción de los equipos tanto dentro como fuera de la organización.
	11.2.2	Servicios de públicos de soporte.	SI	
	11.2.3	Seguridad del cableado.	SI	
	11.2.4	Mantenimiento de los equipos.	SI	
	11.2.5	Retiro de activos.	SI	Se adopta este control, puesto que se requiere dar protección a los activos en cuanto confidencialidad, integridad y disponibilidad, de tal forma, definiendo responsabilidades claras en cuanto a seguridad de la información, con el fin de establecer controles de seguridad para asegurar que se evite el acceso de usuarios no autorizados y el robo de información.
	11.2.6	Seguridad de equipos y activos fuera de las instalaciones (predio).	SI	
	11.2.7	Disposición segura o reutilización de equipos.	SI	
	11.2.8	Equipo de usuario desatendido.	SI	
	11.2.9	Política de escritorio limpio y pantalla limpia.	SI	
12. Seguridad de las Operaciones	**12. Seguridad de las operaciones**			
	12.1	**Procedimientos Operacionales y Responsabilidades.** **Objetivo:** Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.		
	12.1.1	Procedimientos de operación documentados.	SI	Se adopta este control, puesto que se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamientos de información que afectan la seguridad de la información. Se debe hacer seguimiento al uso de los recursos, hacer los ajustes y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema
	12.1.2	Gestión de cambios.	SI	
	12.1.3	Gestión de capacidad.	SI	
	12.1.4	Separación de los ambientes de desarrollo, pruebas, y operacionales.	SI	

Cuadro 19. (Continuación)

ISO 27001:2005 Controles – Anexo A			Aplica (SI/NO)	Justificación
Dominio	**Sección**	**Control**		
12. Seguridad de las Operaciones	**12.2**	**Protección contra Códigos Maliciosos.** **Objetivo:** Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.		
	12.2.1	Controles contra códigos maliciosos.	SI	Se adopta este control, puesto que se debe implementar controles de detección, de prevención y de recuperación, combinados con la implementación de procedimientos de revisión de virus, troyanos o cualquier paquete o archivo que pueda afectar la seguridad de la información.
	12.3	**Copias de Respaldo.** **Objetivo:** Proteger contra la pérdida de datos.		
	12.3.1	Copias de respaldo de la información.	SI	Se adopta este control, puesto que se deben hacer copias de respaldo de la información, software e imágenes de los diferentes sistemas de información. De igual forma se deben realizar pruebas regularmente de acuerdo con una política de copias de respaldo.
	12.4	**Registro y Seguimiento.** **Objetivo:** Registrar eventos y generar evidencia.		
	12.4.1	Registro de eventos.	SI	Se adopta este control, puesto que es importante establecer controles de seguridad que permitan la detección oportuna de actividades de procesamiento de información no autorizadas y herramientas para investigaciones futuras de incidentes de seguridad de la información
	12.4.2	Protección de la información de registro.	SI	
	12.4.3	Registros del administrador y del operador.	SI	
	12.4.4	Sincronización de Relojes.	SI	
	12.5	**Control de software operacional.** **Objetivo:** Asegurarse de la integridad de los sistemas operacionales.		
	12.5.1	Instalación de software en sistemas operativos.	SI	Se adopta este control, puesto que se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.

Cuadro 19. (Continuación)

ISO 27001:2005 Controles – Anexo A			Aplica (SI/NO)	Justificación
Dominio	**Sección**	**Control**		
12. Seguridad de las Operaciones	**12.6**	**Gestión de la Vulnerabilidad Técnica.** **Objetivo:** Prevenir el aprovechamiento de las vulnerabilidades técnicas.		
	12.6.1	Control de las vulnerabilidades técnicas.	SI	Se adopta este control, puesto que se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información; de igual forma se debe evaluar la exposición de la organización a esas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
	12.6.2	Restricciones sobre la instalación de software.	SI	
	12.7	**Consideraciones sobre auditorías de sistemas de Información.** **Objetivo:** Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.		
	12.7.1	Controles sobre auditorías de sistemas de Información.	SI	Se adopta este control, puesto que es importante establecer controles de seguridad que garanticen un que se cuenta con herramientas de auditoría en los sistemas de información críticos, con el objetivo de identificar posibles riesgos asociados a fuga y pérdida de la información.
13. Seguridad de las Comunicaciones	**13. SEGURIDAD DE LAS COMUNICACIONES**			
	13.1	**Gestión de la Seguridad de las Redes.** **Objetivo:** Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.		
	13.1.1	Controles de redes.	SI	Se adopta este control, puesto que es importante establecer controles de seguridad para asegurar la información en la red, protegerla de amenazas y garantizar su infraestructura de soporte.
	13.1.2	Seguridad de los servicios de la red.	SI	
	13.1.3	Separación en las redes.	NO	En la red de Combustibles Líquidos no aplica este control, No se requiere este control para la protección de la información.
	13.2	**Transferencia de Información.** **Objetivo:** Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.		
	13.2.1	Políticas y procedimientos de transferencia de información.	SI	Se adopta este control, puesto que se debe contar con políticas, procedimientos y controles de transferencia segura de archivos para proteger la información. De igual forma se debe proteger los mensajes electrónicos, para que no pierdan su confidencialidad, integridad y disponibilidad.
	13.2.2	Acuerdos sobre transferencia de información	SI	
	13.2.3	Mensajes electrónicos.	SI	
	13.2.4	Acuerdos de confidencialidad o de no divulgación.	SI	Mediante la política de seguridad de la información se establece el compromiso, organización y asignación de responsabilidades para la seguridad de la información, por lo tanto se deben tener acuerdos de confidencialidad.

Cuadro 19. (Continuación)

ISO 27001:2005 Controles – Anexo A			Aplica (SI/NO)	Justificación
Dominio	**Sección**	**Control**		
14. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	**14. Adquisición, desarrollo y mantenimiento de sistemas de información**			
	14.1	**Requisitos de Seguridad de los Sistemas de Información.** **Objetivo:** Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.		
	14.1.1	Análisis y especificación de requisitos de seguridad de la información.	SI	Se adopta este control, dado que es necesario establecer controles de seguridad para garantizar que se tienen en cuenta los requisitos del negocio antes de implementar cambios en la tecnología de la empresa.
	14.1.2	Seguridad de servicios de las aplicaciones en redes públicas.	SI	
	14.1.3	Protección de transacciones de servicios de aplicaciones.	SI	
	14.2	**Seguridad en los Procesos de Desarrollo y Soporte.** **Objetivo:** Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.		
	14.2.1	Política de desarrollo seguro.	NO	En Combustibles Líquidos de Colombia no se desarrollan aplicaciones, por lo tanto este control no aplica.
	14.2.2	Procedimientos de control de cambios en sistemas.	SI	Se adopta este control, puesto que se deben establecer y aplicar reglas para el paso a producción de nuevas versiones de los diferentes sistemas de información, contemplados dentro del ciclo de vida de las aplicaciones.
	14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operaciones.	SI	
	14.2.4	Restricciones sobre cambios en los paquetes de software.	SI	
	14.2.5	Principios de organización de sistemas seguros.	SI	
	14.2.6	Ambiente de desarrollo seguro.	NO	En Combustibles Líquidos de Colombia no se desarrollan aplicaciones, por lo tanto este control no aplica.
	14.2.7	Desarrollo de software contratado	NO	

Cuadro 19. (Continuación)

ISO 27001:2005 Controles – Anexo A			Aplica (SI/NO)	Justificación
Dominio	**Sección**	**Control**		
14. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	14.2.8	Pruebas de seguridad de sistemas.	SI	Se adopta este control, puesto que durante el mantenimiento de sistemas se deben llevar a cabo pruebas de aceptación de nuevas funcionalidades.
	14.2.9	Prueba de aceptación de sistemas.	SI	
	14.3	**Datos de Prueba.** **Objetivo:** Asegurar la protección de los datos usados para pruebas.		
	14.3.1	Protección de datos de prueba.	SI	Se adopta este control, puesto que los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.
15. Relaciones con los Proveedores	**15. Relaciones con los proveedores**			
	15.1	**Seguridad de la información en las relaciones con los proveedores.** **Objetivo:** Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.		
	15.1.1	Política de seguridad de la información para las relaciones con proveedores.	SI	Se adopta este control, puesto que se debe garantizar que se tengan en cuenta los requisitos del negocio antes de gestionar compras de bienes o servicios que afecten la seguridad de la información de la organización y la infraestructura requerida para el desarrollo de los procesos.
	15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores.	SI	
	15.1.3	Cadena de suministro de tecnología de información y comunicación.	SI	
	15.2	**Gestión de la prestación de servicios de proveedores.** **Objetivo:** Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.		
	15.2.1	Seguimiento y revisión de los servicios de los proveedores	SI	Se adopta este control, puesto que se debe garantizar que se tengan en cuenta los requisitos del negocio antes de gestionar compras de bienes o servicios que afecten la seguridad de la información de la organización y la infraestructura requerida para el desarrollo de los procesos.
	15.2.2	Gestión de cambios a los servicios de los proveedores	SI	

Cuadro 19. (Continuación)

ISO 27001:2005 Controles – Anexo A			Aplica (SI/NO)	Justificación
Dominio	**Sección**	**Control**		
16. Gestión de Incidentes de Seguridad de la Información	**16. Gestión de incidentes de seguridad de la información**			
	16.1	**Gestión de incidentes y mejoras en la seguridad de la información.** **Objetivo:** Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.		
	16.1.1	Responsabilidades y procedimientos.	SI	Se adopta este control, dado que es necesario que los activos de información sean sometidos a análisis, evaluación y tratamiento de posibles riesgos a los cuales pueden ser objeto. De igual forma se adopta este control, puesto que se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información
	16.1.2	Informe de eventos de seguridad de la información.	SI	
	16.1.3	Informe de debilidades de seguridad de la información.	SI	
	16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	SI	
	16.1.5	Respuesta a incidentes de seguridad de la información.	SI	
	16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información.	SI	
	16.1.7	Recolección de evidencias.	SI	
17. Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio.	**17. Aspectos de seguridad de la información de la gestión de continuidad de negocio.**			
	17.1	**Continuidad de seguridad de la información.** **Objetivo:** La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.		
	17.1.1	Planificación de la continuidad de la seguridad de la información.	SI	Se adopta este control, puesto que es necesario para que la organización pueda dar continuidad a los procesos misionales. Se debe determinar los requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en los diferentes escenarios en donde se puedan presentar fallas o interrupciones por situaciones adversas, por ejemplo, durante una crisis o desastre.
	17.1.2	Implementación de la continuidad de la seguridad de la información.	SI	
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	SI	
	17.2	**Redundancias** **Objetivo:** Asegurarse de la disponibilidad de instalaciones de procesamiento de información.		
	17.2.1	Disponibilidad de instalaciones de procesamiento de información.	SI	Se adopta este control, puesto que en Combustibles Líquidos de Colombia, las instalaciones procesamiento de la información deben contar con la redundancia suficiente para cumplir los requisitos de disponibilidad.

Cuadro 19. (Continuación)

ISO 27001:2005 Controles – Anexo A			Aplica (SI/NO)	Justificación
Dominio	**Sección**	**Control**		
18. Cumplimiento	**18. Cumplimiento.**			
	18.1	**Cumplimiento de requisitos legales y contractuales.** **Objetivo:** Evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.		
	18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales.	SI	Se adopta este control, puesto que todos los requisitos legales, reglamentarios y contractuales se deben identificar y documentar explícitamente, para darles cumplimiento. Se deben mantener actualizados para cada sistema de información de la organización.
	18.1.2	Derechos de propiedad intelectual.	SI	
	18.1.3	Protección de los registros.	SI	
	18.1.4	Privacidad y protección de información de datos personales.	SI	
	18.1.5	Reglamentación de controles criptográficos.	SI	Se adopta este control, puesto que se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinente.
	18.2	**Revisiones de seguridad de la información.** **Objetivo:** Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.		
	18.2.1	Revisión independiente de la seguridad de la Información.	SI	Se adopta este control, dado que es necesario identificar las posibles mejoras del sistema de gestión de la seguridad implementado en Combustibles Líquidos de Colombia.
	18.2.2	Cumplimiento con las políticas y normas de seguridad.	SI	Se adopta este control, dado que es importante establecer mecanismos de seguridad que garanticen que todo el personal de la empresa conoce y aplica las políticas de seguridad de la información y los respectivos controles.
	18.2.3	Revisión del cumplimiento técnico.	SI	

Fuente: Autores

7. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La información para Combustibles Líquidos de Colombia S.A. E.S.P es considerada como un activo que tiene valor, y por consiguiente debe ser debidamente protegida.

Esta política de seguridad de la Información, busca la protección de los recursos y la información, de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del negocio de la compañía.

Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional y para esto se asegura un compromiso manifiesto de la dirección de Combustibles Líquidos de Colombia S.A. E.S.P para la difusión, consolidación y cumplimiento de la presente política.

Estos lineamientos aplican para todos los empleados, contratistas, consultores, personal temporal y cualquier otra persona que trabaje en o para Combustibles Líquidos de Colombia S.A. E.S.P. Incluyendo a todo el personal de terceros y toda la infraestructura que sea poseída, alquilada y/o operada por Combustibles Líquidos de Colombia S.A. E.S.P.

Rubén Darío Espitia Manrique
Coordinador de Tecnología

Carlos Alcalá Payares
Director de Tecnología

Willinton Ayala Mosquera
Gerente General Combustibles Líquidos de Colombia S.A. ESP

7.1 OBJETIVO

Combustibles Líquidos de Colombia S.A. E.S.P. establece, define y revisa unos objetivos dentro de sus sistemas de información, encaminados a mejorar su seguridad, entendiéndola como la conservación de la confidencialidad, integridad y disponibilidad de su información, así como la de la infraestructura que la soportan, con el objetivo de aumentar la confianza de sus clientes, accionistas y demás partes interesadas.

El diseño, implantación y mantenimiento de estas políticas se apoya en los resultados de un proceso continuo de análisis y gestión de riesgo del que se derivan

las actividades a desarrollar en materia de seguridad dentro del alcance de su sistema que es “seguridad de la información en el proceso de Infraestructura TI, en Combustibles Líquidos de Colombia S.A. E.S.P.”.

La dirección de Combustibles Líquidos de Colombia S.A. E.S.P. se compromete a apoyar y mantener las políticas de seguridad de la información. Para ello la compañía implantará las medidas requeridas para la formación y concientización del personal respecto a la seguridad de la información. Adicionalmente, cuando cualquier funcionario incumpla las políticas de seguridad, la dirección se reserva el hecho de aplicar las medidas disciplinarias acordes aplicables y dimensionadas al impacto que tengan sobre la organización.

7.2 ALCANCE

Con el ánimo de mejorar la estrategia de Seguridad de la información de Combustibles Líquidos de Colombia, se diseñó con la ayuda de la jefatura de sistemas, la siguiente política de seguridad de la información, con la cual se busca aplicar un modelo base que permita alinear los procesos hacia un mismo objetivo de seguridad en el manejo de la información.

La política permite establecer un marco de trabajo de la organización en lo referente al uso adecuado de los recursos, para la búsqueda de niveles adecuados de protección y resguardo de la información, a través de lineamientos, para garantizar el debido control y minimizar los riesgos asociados.

7.3 TÉRMINOS Y DEFINICIONES

En el desarrollo de estos lineamientos se utilizan los siguientes términos y definiciones presentados en la norma ISO/IEC 27001:2013, a continuación se enumeran solo los que son necesarios para entender el presente documento:

- Control de Acceso: medios utilizados para asegurar que el acceso a los activos está autorizado y restringido, basado en unos requerimientos de negocio y de seguridad.

- Auditoría: proceso sistemático, independiente y documentado que permite obtener evidencias y evaluarlas de manera objetiva para determinar el nivel de cumplimiento frente a una norma, estándar, políticas y/o procedimientos de Combustibles Líquidos de Colombia S.A. ESP. Una auditoría puede ser interna (realizada por personal de Combustibles Líquidos de Colombia S.A. ESP) o externa (realizada por personal ajeno a la entidad).

- Disponibilidad: propiedad de ser accesible y utilizable bajo la demanda de una individuo o proceso autorizado.

- Competencia: habilidad de aplicar el conocimiento y las habilidades con las que se cuenta para lograr un objetivo esperado.

- Confidencialidad: propiedad que garantiza que la información no está disponible o no es divulgada a individuos o procesos no autorizados.

- Mejora continua: actividad recurrente que mejora el desempeño.

- Control: medida utilizada para disminuir el riesgo.

- Objetivo de control: párrafo que describe que se debe lograr como resultado de implementar un control.

- Corrección: acción tomada para eliminar una no conformidad.

- Acción correctiva: acción tomada para eliminar la causa raíz de una no conformidad y para evitar su recurrencia.

- Información documentada: información que se debe controlar y mantener por Combustibles Líquidos de Colombia S.A. ESP.

- Efectividad: nivel al que las actividades planeadas fueron ejecutadas y al que los resultados planeados fueron cumplidos.

- Alta dirección: grupo de personas que tienen la responsabilidad de implementar las estrategias y políticas necesarias para que la organización cumpla con sus objetivos. En el caso de Combustibles Líquidos de Colombia S.A. ESP la alta dirección está compuesta por los gerentes de cada una de las áreas, liderados por la Gerente General.

- Contexto externo: ambiente externo en el que la organización busca cumplir sus objetivos. Comprende los ambientes cultural, social, político, legal, regulatorio, financiero, tecnológico, económico, natural y competitivo; en escalas internacional, nacional, regional y/o local.

- Contexto interno: ambiente interno en el que la organización busca cumplir sus objetivos. Comprende el gobierno corporativo, la estructura organizacional, las políticas, objetivos y capacidades de la compañía, los sistemas de información, el recurso humano y la cultura de la compañía.

- Instalaciones de procesamiento de información: cualquier sistema, servicio o infraestructura de procesamiento, así como la ubicación física que lo resguarda.

- Integridad: propiedad que permite garantizar la precisión y completitud de la información.

- Parte interesada: persona u organización que puede afectar, ser afectada o percibir ser afectada por las decisiones y/o actividades de Combustibles Líquidos de Colombia S.A. ESP.

- Riesgo: efecto de la incertidumbre sobre los objetivos de Combustibles Líquidos de Colombia S.A. ESP.

7.4 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

7.4.1 Política general. Combustibles Líquidos de Colombia S.A. E.S.P. establece, define y revisa unos objetivos dentro de sus sistemas de información, encaminados a mejorar su seguridad, entendiéndola como la conservación de la confidencialidad, integridad y disponibilidad de su información, así como la de la infraestructura que la soportan, con el objetivo de aumentar la confianza de sus clientes, accionistas y demás partes interesadas.

El diseño, implantación y mantenimiento de estas políticas se apoya en los resultados de un proceso continuo de análisis y gestión de riesgo del que se derivan las actividades a desarrollar en materia de seguridad dentro del alcance de su sistema que es “seguridad de la información en el proceso de Infraestructura TI, en Combustibles Líquidos de Colombia S.A. E.S.P.”.

La dirección de Combustibles Líquidos de Colombia S.A. E.S.P. se compromete a apoyar y mantener las políticas de seguridad de la información. Para ello la compañía implantará las medidas requeridas para la formación y concientización del personal respecto a la seguridad de la información. Adicionalmente, cuando cualquier funcionario incumpla las políticas de seguridad, la dirección se reserva el hecho de aplicar las medidas disciplinarias acordes aplicables y dimensionadas al impacto que tengan sobre la organización.

Directrices: Todos los colaboradores de Combustibles Líquidos de Colombia S.A. ESP tienen la responsabilidad de cumplir con los lineamientos de seguridad de la información. Los lineamientos se actualizarán de forma anual o cada vez que hayan cambios importantes sobre el SGSI.

Los colaboradores de Combustibles Líquidos de Colombia S.A. ESP deben leer las actualizaciones de los lineamientos y familiarizarse con aquellos cambios que puedan impactar sus funciones.

Aplicabilidad: Estas son políticas que aplican a la alta dirección, directores, jefes de área, funcionarios, contratistas, y en general a todos los usuarios de la información en Combustibles Líquidos de Colombia.

7.4.2 Organización de la seguridad de la información. Cada colaborador de Combustibles Líquidos de Colombia S.A. ESP debe tener un rol definido para la seguridad de la información, de tal forma que pueda desempeñar su actividad laboral y cumplir a cabalidad con los requerimientos de la empresa.

A continuación se definen los roles y responsabilidades que deben ser desempeñadas por los colaboradores frente a la seguridad de la información:

7.4.2.1 Alta dirección. La alta dirección debe revisar y aprobar la política de seguridad de la información, por lo menos una vez al año, o cuando ocurra algún cambio significativo en la organización. De igual forma debe:

- Asegurar que los requisitos del SGSI se encuentran integrados en los procesos de la organización.

- Asegurar que el SGSI cuente con los recursos necesarios para su correcta operación.

- Comunicar la importancia de una gestión de la seguridad de la información eficaz y de la conformidad con los requisitos del SGSI.

- Asegurar que el SGSI logre los resultados previstos.

- Dirigir y apoyar a las personas, para contribuir a la eficacia del SGSI.

- Promover la mejora continua.

7.4.2.2 Oficial de seguridad de la información. Las principales responsabilidades de este rol incluyen pero no se limitan a:

- Propiciar, sugerir y diseñar el desarrollo de estrategias para la mitigación de los riesgos detectados.

- Velar por el cumplimiento de las políticas corporativas, lineamientos locales y regulaciones del SGSI.

- Evaluar la utilización y la efectividad de los recursos de seguridad de la información.

- Desarrollar e implementar diferentes métricas de seguridad para medir la efectividad del SGSI.

- Dirigir y revisar las actividades de seguridad de la información de Combustibles Líquidos de Colombia S.A. ESP.

- Analizar las alertas globales de seguridad y determinar los planes de acción que deben seguirse para tratamiento a las mismas.

- Establecer y mantener el marco de trabajo del SGSI y desarrollar estrategias de seguridad que deberán ser usadas como base para proveer controles de seguridad de la información y procedimientos que se requieran.

- Participar en el mejoramiento continuo del SGSI.

- Asegurarse de que el SGSI de Combustibles Líquidos de Colombia S.A. ESP esté implementado en conformidad con los requisitos de la norma ISO27001:2013.

- Informar a la alta dirección sobre el desempeño del SGSI.

7.4.2.3 Director de tecnología. Las principales responsabilidades de este rol incluyen pero no se limitan a:

- Garantizar el cumplimiento de las políticas y lineamientos de seguridad, así como los estándares y procedimientos que gobiernan el área de tecnología.

- Garantizar la confidencialidad, integridad y disponibilidad de la información que se encuentra en los diferentes sistemas de información.

- Trabajar conjuntamente con el oficial de seguridad de la información en el establecimiento de planes de continuidad de negocio y recuperación ante desastres.

- Trabajar conjuntamente con el oficial de seguridad de la información en el diseño e implementación de controles tecnológicos que ayuden a mitigar los riesgos identificados.

- Garantizar una adecuada gestión de los incidentes de seguridad reportados dentro de su área.

7.4.2.4 Director de recursos humanos. Las principales responsabilidades de este rol incluyen pero no se limitan a:

- Garantizar la seguridad de la información personal entregada por los colaboradores durante su proceso de vinculación y trabajo en la compañía.

- Trabajar conjuntamente con los gerentes y/o responsables de área para el desarrollo y definición de los roles y responsabilidades para cada cargo.

- Incorporar las responsabilidades específicas sobre la seguridad de la información en todas las descripciones de cargo y contratos de los trabajadores o terceros.

- Incluir el cumplimiento de las políticas y procedimientos relacionados con seguridad de la información en todas las evaluaciones de desempeño de los colaboradores.

- Trabajar conjuntamente con los gerentes o dueños de proceso para el establecimiento de acciones disciplinarias (con base en el reglamento interno de trabajo) cuando se detecten violaciones al SGSI.

- Informar a los trabajadores sobre la existencia de peligros en el sitio de trabajo, suministrar medidas de seguridad para minimizar el riesgo a los trabajadores y adiestrar a los trabajadores en el uso apropiado de las medidas de seguridad. Esta actividad debe ejecutarse como mínimo una vez al año.

7.4.2.5 Propietario - Responsable de los activos. Las principales responsabilidades de este rol incluyen pero no se limitan a:

- Asignar la clasificación inicial a la información y revisarla periódicamente para asegurar que cumple los requerimientos del negocio.

- Asegurar que los controles de seguridad sean implementados de acuerdo al nivel de clasificación de la información.

- Revisar y asegurar los privilegios de acceso asociados con los activos de información que es responsable.

- Determinar los requerimientos de seguridad, criterios de acceso y criterios de copias de respaldo para los activos de información de los que es responsable.

7.4.2.6 Custodio del activo. Las principales responsabilidades de este rol incluyen pero no se limitan a:

- Garantizar que la información que le ha sido confiada sea protegida durante todo su ciclo de vida (creación, almacenamiento, distribución, transporte y destrucción) de modificaciones y usos no autorizados.

- Garantizar la confidencialidad, integridad y disponibilidad de la información que le ha sido confiada.

- Asegurar que los requerimientos de retención de registros estén basados en los análisis realizados por el responsable de la información.

7.4.2.7 Todos los usuarios. Las principales responsabilidades de todos los usuarios, incluyen pero no se limitan a:

- Cumplir todas aquellas responsabilidades que han sido consignadas en las políticas de seguridad corporativas y lineamientos de seguridad locales.

.

- Proteger la información que Combustibles Líquidos de Colombia S.A. ESP le ha suministrado para la ejecución de sus labores.

- Firmar un acuerdo de confidencialidad y/o no divulgación antes de iniciar formalmente sus labores dentro de la compañía,

- Reconocer que la propiedad intelectual incluyendo sin limitantes, patentes, derechos de autor, marcas registradas y todos los otros derechos de propiedad intelectual tal como se manifiestan en memorandos, planes, estrategias, productos, programas de computación, documentación y demás material desarrollado o concebido mientras el colaborador esté desarrollando sus labores o gestión en sitios alternativos de trabajo, son exclusiva propiedad de Combustibles Líquidos de Colombia S.A. ESP.

- Mantener la confidencialidad de sus contraseñas.

- Garantizar la seguridad de la información que está bajo su cuidado.

- Usar los activos de la compañía y los recursos de información de manera segura y adecuada para desempeñar sus funciones laborales.

7.4.2.8 Terceros. Todo contratista, consultor, proveedor o cliente que tenga acceso a la información de Combustibles Líquidos de Colombia S.A. ESP tiene los mismos deberes que un colaborador o un prestador de servicios de Combustibles Líquidos de Colombia S.A. ESP frente a la protección de la información que le ha sido suministrada.

7.4.3 Lineamientos para dispositivos móviles

Objetivo: Establecer las directrices para el uso y manejo adecuado de dispositivos móviles y equipos de terceros.

Directrices:

- Los laptops, tablets, Smartphone, memorias USB y otros dispositivos móviles deben estar protegidos mediante una contraseña y tener la función de cifrado de datos habilitada.

- Tener habilitada la función de bloqueo por inactividad.

- Protegerse en todo momento, evitando dejarlos desatendidos en áreas públicas.

- Cuando un colaborador de Combustibles Líquidos de Colombia S.A. ESP viaje con dispositivos móviles que contengan información de la compañía:

  - No debe utilizar las funciones “suspender” o “hibernar” de su computador portátil, se debe cerrar la sesión y apagar el equipo.

  - Debe llevar sus dispositivos portátiles como equipaje de mano, estos elementos jamás deben transportarse en la bodega.

  - Debe reportar al oficial de seguridad en caso de pérdida del equipo.

  - No se debe exponer a peligros físicos en caso de ser abordado por un ladrón.

- La instalación de aplicaciones en los computadores portátiles por parte de los colaboradores está prohibida, todos los requerimientos de instalación deben hacerse al área de tecnología, quien será la encargada de realizar el proceso.

- No se deben instalar aplicaciones de fuentes desconocidas en los dispositivos móviles como celulares o tablets. Si los colaboradores tienen alguna duda respecto a alguna aplicación en particular, deben contactar al oficial de seguridad de la información quien dará su apoyo y concepto al respecto.

7.4.4 Políticas de seguridad para los recursos humanos

Objetivo: Definir los lineamientos que se deben aplicar a la gestión del recurso humano, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información.

Directrices antes de asumir el empleo:

- El ofrecimiento formal de empleo debería hacerse sólo al personal que obtuvo resultados satisfactorios en las diferentes verificaciones requeridas por Combustibles Líquidos de Colombia S.A. ESP.

- Antes de iniciar sus labores dentro de la compañía, los colaboradores que fueron escogidos durante el proceso de selección, deben firmar su contrato de trabajo como aceptación de los términos y condiciones de empleo que van a desempeñar. El contrato o sus anexos deben contemplar las responsabilidades frente a la seguridad de la información para el nuevo trabajador, incluyendo en él una clausula en donde se le prohíba al empleado el almacenamiento de información sensible y reservada del mismo en los equipos de la compañía.

- Los colaboradores deben firmar acuerdos de confidencialidad antes que se les otorgue acceso a las instalaciones de procesamiento y/o acceso a la información de Combustibles Líquidos de Colombia S.A. ESP o de terceros.

Directrices durante la ejecución del empleo:

- Debe comunicarse al nuevo trabajador, contratista y/o tercero sus responsabilidades y derechos legales (Ej., derechos de autor, patentes, uso apropiado de activos, clasificación y manejo de información, horarios laborales, políticas y lineamientos de seguridad, etc.)

- La dirección de recursos humanos debe realizar cada año la verificación de antecedentes judiciales para todos los colaboradores, contratistas y terceros con Combustibles Líquidos de Colombia S.A. ESP que tengan acceso a información confidencial.

- Combustibles Líquidos de Colombia S.A. ESP exigirá a sus colaboradores el cumplimiento de todos los lineamientos de seguridad de la información.

- Todos los colaboradores recibirán la educación y formación necesaria para generar conciencia respecto a la seguridad de la información.

- La dirección de recursos humanos comunicará a los colaboradores el proceso disciplinario que se aplicará cuando se incumplan los lineamientos de seguridad de la información.

Directrices para la terminación y cambio de empleo:

- Se deben definir y asignar claramente las responsabilidades para realizar la terminación o cambio del empleo ya sea que el retiro sea voluntario o no voluntario.

- En el momento que cualquier colaborador termine su relación contractual con Combustibles Líquidos de Colombia S.A. ESP, toda propiedad y/o activo de la compañía debe ser devuelta al supervisor inmediato y/o a la coordinación de tecnología. Esta entrega debe quedar formalmente registrada mediante formato que en el momento de la entrega se encuentre avalado por el área de calidad.

7.4.5 Política de gestión de activos de información

Objetivo: Establecer las directrices para mantener la protección adecuada de los activos de información.

Directrices:

- Todo activo que esté contemplado dentro del alcance del SGSI, debe tener designado un responsable para determinar el custodio, sensibilidad, criticidad, tiempo de retención y controles adecuados para el acceso, almacenamiento, manejo, distribución y uso regular de la información.

- El responsable de los activos o el colaborador que este designé, debe recopilar y mantener permanentemente actualizado un inventario de activos de información en el que deben estar claramente identificadas todas sus características, así como su custodio, ubicación, clasificación y criticidad. Esta revisión debe realizarse con una periodicidad semestral.

- Los “dueños-responsables” de los activos de información en Combustibles Líquidos de Colombia S.A. ESP, deberán garantizar que todos los individuos designados para la administración, uso, diseño, desarrollo, mantenimiento y operación de activos actúen con la debida diligencia según lo establecido en las Políticas, lineamientos de seguridad y sus procedimientos asociados.

- El responsable de los activos debe mantener un listado de los productos y fabricantes autorizados para el desarrollo o adquisición de nuevos sistemas.

- Todo el hardware y software debe obtenerse siguiendo los procedimientos establecidos para tal fin.

- Los activos que Combustibles Líquidos de Colombia S.A. ESP pone a disposición de sus colaboradores sólo deben ser utilizados para desempeñar funciones asociadas con su rol.

- Se deben hacer firmar actas de entrega al directo responsable por cada equipo de cómputo, celular, modem, cámara, scanner, impresora o cualquier otro equipo tecnológico. Este a su vez deberá responder por la integridad física del mismo y la información contenida en este (Dichas actas deben ejecutarse sobre los formatos avalados y publicados por la gerencia y el área de calidad).

- Todos los empleados deben devolver a la coordinación de Tecnología y/o Dirección de Tecnología todos los equipos pertenecientes a la organización que estén en su poder al finalizar el vínculo laboral contrato o acuerdo a través de los formatos avalados.

- Se debe reportar la pérdida o daño los elementos tecnológicos en el menor tiempo posible al director de área correspondiente y este informará posteriormente al área de tecnología. En caso de pérdida el funcionario asumirá el valor.

7.4.6 Políticas de clasificación de la información

Objetivo: Asegurar que la información recibe un nivel de protección apropiado de acuerdo al tipo de clasificación establecido por la ley.

Directrices:

- Toda la información de Combustibles Líquidos de Colombia S.A. E.S.P debe ser clasificada y deben establecerse procedimientos distintos para manejar, etiquetar y revisar cada clasificación.

- Esta política suministra información a todos los funcionarios para guiar el manejo de la seguridad de la información sensible de la compañía.

- Las medidas de protección que deben aplicarse a la información de Combustibles Líquidos de Colombia S.A. ESP dependen de la clasificación asignada a la misma, de acuerdo a los siguientes niveles:

    - Confidencial: Es toda información propia de la alta gerencia extremadamente sensible, su divulgación podría ocasionar serios impactos, como pérdida de

imagen, pérdidas financieras, pérdida de confianza en inversionistas. Ejemplo: estrategia de mercadeo del próximo mes.

- Restringido: Se aplica a información personal que se ha de usar en la compañía. Su divulgación no autorizada podría impactar seria y negativamente a sus empleados, clientes, socios, etc. Ejemplo: listado de nómina.

- Interna: Se aplica a información propia que se ha de usar al interior de Combustibles Líquidos de Colombia S.A. E.S.P. Su divulgación no autorizada podría impactar levemente a la compañía. Ejemplo: publicación de los procedimientos internos.

- Pública: Es toda la información que se encuentra a libre disposición de las personas, sean éstas empleados, clientes, socios comerciales, medios de comunicación, etc. La divulgación de información pública es consistente con la política y no impactará negativamente a Combustibles Líquidos de Colombia S.A. E.S.P, sus empleados, sus accionistas, socios de negocios o sus clientes. Ejemplo: campañas de publicidad.

- Cualquier información que no esté clasificada debe ser tratada como si fuera “Confidencial”.

- Los dueños/creadores de cualquier tipo de información deben revisar su clasificación durante todas las actualizaciones que se realicen sobre la misma.

- Antes de divulgar información confidencial de Combustibles Líquidos de Colombia S.A. ESP o recibir información confidencial de terceras partes, debe firmarse un acuerdo de confidencialidad entre las partes.

7.4.7 Política de control de acceso

Objetivo: Definir los lineamientos para asegurar el acceso físico o lógico, a la información, aplicaciones y/o plataforma de Combustibles Líquidos de Colombia S.A. ESP.

Directrices:

- Cada funcionario dentro de la compañía deberá contar con privilegios y accesos a los diferentes sistemas de información e información de acuerdo a su rol desempeñado dentro de la compañía.

- La autorización o rechazo para el acceso a un activo debe ser dada por el propietario del activo.

- Si un colaborador requiere acceso a un sistema de información o información diferente a los que tiene acceso de acuerdo a su rol debe seguir los procedimientos establecidos para la gestión de usuarios y contraseñas.

- Todo acceso a una base de datos, debe ser controlado a través de un proceso de autenticación.

- Todo el personal interno, externo y contratistas, deben siempre portar de forma visible su carné de identificación de acceso mientras se encuentran dentro de las instalaciones de Combustibles Líquidos de Colombia S.A. ESP

- El préstamo del carné y/o tarjeta de acceso se encuentra prohibido.

- Todos los empleados y/o terceros que así lo requieran, tendrán un nombre de usuario y una contraseña que servirán para identificarlos y permitirles el acceso a los sistemas de Combustibles Líquidos de Colombia S.A. ESP.

- Cada colaborador y/o tercero es responsable por cualquier acción que pueda ejecutarse con su nombre de usuario y será objeto de acciones disciplinarias si se comprueba que ha ocurrido un incidente de seguridad por el uso indebido del mismo.

- Todos los colaboradores y terceros deben proteger correctamente su nombre de usuario y contraseña.

- Está prohibido el uso compartido de cuentas de acceso.

- El acceso a los sistemas de información de Combustibles Líquidos de Colombia S.A. ESP y a las áreas seguras deben ser autorizados por el responsable de acuerdo al rol desempeñado.

- Ningún tercero debe tener acceso a los sistemas y/o áreas seguras de Combustibles Líquidos de Colombia S.A. ESP sin previa autorización.

- Proteja el acceso a su estación de trabajo cuando esta no se encuentre en uso, asegurando la misma.

- El acceso a sistemas y/o áreas seguras de Combustibles Líquidos de Colombia S.A. ESP está sujeto a revisiones periódicas e individuales.

- Está prohibido divulgar las contraseñas asociadas a las cuentas de acceso.

- Todos los privilegios y derechos de uso de los sistemas deben interrumpirse al momento en que por faltas a las presentes políticas o cuando se conozca la finalización del vínculo laboral. Por tal razón, cada director de área debe notificar inmediatamente al área de tecnología este tipo de situaciones, con el objetivo de aplicar las acciones pertinentes.

- Todos los privilegios y derechos de uso de los sistemas deben suspenderse en el momento que ocurra una pérdida del equipo, por tal razón, el responsable debe reportar al área de tecnología inmediatamente suceda el evento.

- Ningún funcionario de la compañía debe mover, trasladar o reemplazar de lugar un equipo de cómputo a excepción de portátiles, salvo expresa solicitud autorizada por la dirección de tecnología

- Los escritorios deben permanecer limpios y despejados. Esto evita exponer su información a otras personas durante su ausencia, además promueve un mejor ambiente de trabajo.

- Está prohibido el uso o almacenamiento de material obsceno, pornográfico, música o material con fines terroristas, en los equipos o sistemas de información de la compañía.

- Se restringe el uso de internet obedeciendo al rol del área de trabajo, se deben bloquear las páginas de redes sociales, pornografía, consulta de métodos de hacking, descarga de programas o cualquier otro sitio web que se considere una amenaza a la seguridad y productividad laboral.

- Se restringe el uso de memorias USB, CDRW, DVDRW, discos duros portátiles o cualquier otro medio de almacenamiento extraíble.

- Todo el software, como paquetes de ofimática, sistemas operativos, aplicaciones, antivirus debe estar controlado obedeciendo al rol del área dentro de la compañía.

- Está totalmente prohibida la instalación o desinstalación de programas de software salvo aprobación del área de tecnología.

- Los usuarios deben reportar con prontitud todas las alertas de seguridad, advertencias y vulnerabilidades a la coordinación de tecnología, el cual es la única unidad autorizada de la organización que puede definir el curso de acción conveniente para responder a estas alertas.

7.4.8 Política de seguridad física y del entorno

Objetivo: Definir los lineamientos que deben seguir los usuarios y responsables para acceder a las instalaciones y activos físicos de información, con el fin de asegurar una adecuada protección de la información en Combustibles Líquidos de Colombia S.A. ESP.

Directrices:

- Los equipos de impresión y copiado no deben estar ubicados en zonas donde exista información confidencial a no ser que sean requeridos para desempeñar las labores propias del área o del colaborador.

- Se establecen como áreas seguras dentro de la compañía el centro de cómputo primario o data center.

- Todo visitante que ingrese a un área segura debe registrarse en la bitácora de registro de visitantes.

- No debe permitirse al área segura, el ingreso de equipos fotográficos, vídeo-audio (celulares, Smartphone), almacenamiento u otro tipo que registren información.

- No deben hacerse visitas públicas (Atención a clientes, familiares, proveedores, visitas personales, etc.) en las áreas seguras determinadas por la presente política.

- Las instalaciones deben ser discretas y ofrecer un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores, que identifiquen la presencia de actividades de procesamiento de información.

- Las instalaciones de procesamiento deben estar ubicadas en áreas donde exista baja probabilidad de desastres naturales, accidentes serios causados por el hombre, motines y otros problemas relacionados.

- Los materiales peligrosos o combustibles (materiales inflamables) deben ser almacenados en lugares seguros a una distancia prudencial del Centro de Cómputo.

- Deben estar protegido de posibles fallas en el suministro de energía u otras anomalías eléctricas como mínimo con UPS, generadores y puesta a tierra.

- Se deben realizar revisiones de los permisos de acceso a las diferentes áreas de la compañía, con el fin de detectar fallas en la gestión de tarjeta e intentos no autorizados de acceso.

- Los cables de energía deben estar separados de los cables de comunicaciones para evitar interferencias.

- Todas las estaciones de trabajo de escritorio de Combustibles Líquidos de Colombia S.A. ESP, deben asegurarse de tal forma que se impida la manipulación del interior de equipo por personas no autorizadas.

- Los equipos y dispositivos retirados del ámbito de la organización no deben permanecer desatendidos en lugares públicos. Las computadoras personales deben ser transportadas como equipaje de mano en caso de viaje y cada vez que se utilicen deben ser aseguradas físicamente a una superficie sólida a través de una guaya o cable de fijación.

- Debe certificarse que toda la información sensible ha sido adecuadamente removida de cualquier componente del sistema informático utilizado para los negocios de la empresa, antes de entregar los componentes a terceros.

- Todos los empleados de Combustibles Líquidos de Colombia S.A. E.S.P deben conocer los planes y rutas de evacuación así como el procedimiento para el control de incendios.

7.4.9 Política de seguridad de las operaciones

Objetivo: Definir los lineamientos que deben seguirse para la constante operatividad de la información de Combustibles Líquidos de Colombia S.A. ESP.

Directrices:

- Cualquier proceso de cambio que afecte los sistemas de información debe planificarse y evaluarse para garantizar que este se lleve a cabo de la forma más eficiente, siguiendo siempre las pautas y procedimientos establecidos que aseguren la disponibilidad, integridad confidencialidad de los activos de información.

- Cualquier cambio que requiera modificaciones sobre sistemas de información desarrollados y/o mantenidos por Combustibles Líquidos de Colombia S.A. ESP corporación debe ser registrada tanto local como corporativamente a través de los medios establecidos para tal fin.

- Se debe establecer un comité de cambios el cual deberá evaluar la pertinencia desde el punto de vista de negocio y con la ayuda del grupo de asesores la viabilidad

técnica de cada cambio. Posterior a la evaluación el comité de cambios aprobará o rechazará los cambios.

- El comité de cambios estará compuesto por los siguientes funcionarios: Director de Tecnología, Directora de proyectos, Coordinador de Tecnología y el Oficial de Seguridad de la Información.

- El Director de Tecnología ejercerá las funciones de director de cambios y como su reemplazo ejercerá el Oficial de Seguridad de la Información.

- Se deben revisar periódicamente las demandas de capacidad y realizar proyecciones de los futuros requerimientos de capacidad con el fin de garantizar la disponibilidad, integridad, capacidad de procesamiento y almacenamiento adecuados. Estas proyecciones deben tomar en cuenta los nuevos requerimientos de negocios, sistemas y las tendencias actuales para determinar un adecuado plan de crecimiento de los sistemas de información propiedad de Combustibles Líquidos de Colombia S.A. ESP.

- La Dirección de Tecnología debe utilizar la información de capacidad para identificar y evitar potenciales cuellos de botella que podrían plantear una amenaza a la seguridad del sistema o a los servicios del usuario, y planificar una adecuada acción correctiva.

- Debe respaldarse periódicamente toda la información confidencial, sensitiva y/o crítica contenida en los sistemas de computación y las redes de Combustibles Líquidos de Colombia S.A. ESP. Los responsables de la información deben definir cuál información y cuáles equipos deben respaldarse, así como la frecuencia y el método de respaldo que se empleará, en concordancia con los lineamientos indicados en la presente política.

- Para los sistemas de Información en producción se realizará una copia de respaldo diaria.

- Para los equipos de red y seguridad se realizará una copia de respaldo de la configuración cada vez que se realicen modificaciones sobre el mismo. Esta copia de respaldo deberá ser almacenada en una ruta de red definida la cual estará cubierta por el esquema de respaldo diario realizado a los sistemas de información.

- Las copias de respaldo no deben ser almacenadas inmediatamente en la librería de medios sin haber sido rotulada como mínimo con la siguiente información: nombre del sistema de producción, fecha de creación, clasificación de la información, datos de contacto del responsable de las operaciones de copia de respaldo.

- Deben realizarse pruebas a las copias de respaldo como mínimo una vez al año, para asegurar que pueden ser restaurados completamente durante todo el periodo de conservación.

- Las copias de respaldo deberán ser enviadas a custodia externa para garantizar la integridad y disponibilidad de las cintas de acuerdo a los parámetros establecidos por el fabricante de las mismas.

- La revisión de los registros y otra información generada por los diferentes sistemas de información debe realizarse de forma periódica por parte de los custodios de los diferentes sistemas como parte de sus actividades de gestión de administración de los mismos.

- Cualquier excepción o incidente de seguridad descubierta dentro de las diferentes revisiones de los sistemas y/o redes, debe ser registrado y gestionado a través del procedimiento de gestión de incidentes

- El personal autorizado para revisar los registros de auditoría de los diferentes sistemas no debe divulgar esta información sin previa autorización del Director de Tecnología y el Oficial de Seguridad.

- Cualquier excepción o incidente de seguridad descubierto durante la revisión de un sistema o componente de red, debe ser reportado a través del procedimiento de gestión de incidentes de seguridad.

- Los registros electrónicos que son creados como resultado del seguimiento y rastreo de actividades del sistema y del tráfico de red, deben ser protegidos y retenidos por el tiempo que estipule la legislación Colombiana aplicable, regulación local o acuerdo contractual establecido.

- Las pruebas de seguridad a los activos críticos de la compañía deben ejecutarse como mínimo una vez por año o cada vez que se presenten las siguientes situaciones:

    - Modificación mayor de la configuración de un sistema en producción.

    - Adición de un nuevo sistema a la infraestructura de tecnología de Combustibles Líquidos de Colombia S.A. ESP (Temporal o permanente).

    - Modificación de la topología de red sobre la cual el sistema se encuentre conectado.

- Toda tarea de mitigación de hallazgos y vulnerabilidades debe ser evaluada regularmente para garantizar la efectividad y eficiencia del control.

- La mitigación de vulnerabilidades y hallazgos con criticidad alta, deben ser tratados con prioridad sobre los hallazgos con criticidad media y baja.

- Se deben realizar auditorías internas como mínimo una vez al año al Sistema de Gestión de Seguridad de la Información.

- Los requerimientos y actividades de auditoría que involucren verificaciones de los sistemas en producción deben ser cuidadosamente planificados y acordados con el fin de minimizar el riesgo de discontinuidad de los procesos de negocio.

- Los requerimientos de auditoría deben ser acordados con la gerencia del área auditada.

- Se debe acordar y controlar el alcance de las verificaciones.

- Estas deben estar limitadas a un acceso de sólo lectura del software de datos.

- El acceso que no sea de sólo lectura solamente debe permitirse para copias aisladas de archivos del sistema, las cuales deben ser eliminadas una vez finalizada la auditoría.

- Se deben identificar claramente y poner a disposición los recursos de tecnología de la información para llevar a cabo las verificaciones.

- Se deben identificar y acordar los requerimientos de procesamiento especial o adicional.

- Todos los accesos deben ser monitoreados y registrados con el fin de generar un registro.

- Los resultados obtenidos en las auditorías realizadas deben ser comunicados a la gerencia general y al representante ante la dirección.

- Debe realizarse un plan de tratamiento de los hallazgos encontrados en las auditorías internas y/o externas. Este plan debe contemplar como mínimo los tiempos de ejecución, impacto de la actividad, responsables, recursos y fechas de implementación.

- Una vez tratados los hallazgos y mitigadas las vulnerabilidades, el representante ante la dirección debe dar respuesta al informe de auditoría en cuestión.

- En los sistemas de comunicación que la compañía ha adoptado utilizar, en especial el correo electrónico, debe usarse únicamente para actividades empresariales, se debe evitar el uso irresponsable como reenviar cadenas de correo, spam, publicidad o lenguaje obsceno que interfiera con la productividad del trabajador y no tenga prioridad sobre otras actividades del negocio.

- Debe asegurarse que las actualizaciones automáticas de su equipo estén habilitadas. Al hacer que el sistema operativo este actualizado disminuye la probabilidad de que ocurra un ataque de virus o código malicioso sobre su máquina.

7.4.10 Política contra código malicioso

- Debe establecerse las medidas de seguridad necesarias para garantizar que la Información que pudiese almacenarse por requerimientos del negocio se encuentre libre de software malicioso.

- Debe establecerse los controles de seguridad adecuados para evitar la instalación en equipos de cómputo, servidores, equipos de red y comunicaciones de programas o dispositivos que capturen la información de sus clientes y de sus operaciones.

- Debe establecerse los mecanismos necesarios para que el mantenimiento y la instalación o desinstalación de programas o dispositivos en las terminales o equipos de cómputo solo lo pueda realizar personal debidamente autorizado.

- Debe mantenerse ambientes independientes para actividades de pruebas, desarrollo y producción. En todo caso, el desempeño y la seguridad de un ambiente no podrán influir en los demás.

- Debe establecerse procedimientos que permitan verificar que las versiones de los programas del ambiente de producción corresponden a las versiones de programas fuentes catalogadas.

- Debe establecerse los procedimientos y controles para el paso de programas o servicios a producción. El software en operación deberá estar catalogado.

- Debe mantenerse actualizados todos los diagramas de las conexiones y flujos de datos que salen o entran hacia los ambientes de producción.

- Debe mantenerse documentada y actualizada toda la información referente a los parámetros de los sistemas donde operan las aplicaciones en producción, incluido el ambiente de comunicaciones; versión de los programas y aplicativos en uso;

soportes de las pruebas realizadas a los sistemas de información; y procedimientos de instalación del software.

- Debe definirse los procedimientos y medidas que se ejecutarán cuando se encuentre evidencia de la alteración de los dispositivos utilizados en el servicio de corresponsal no bancario.

7.4.11 Política de uso de contraseñas

Objetivo: Definir los lineamientos que deben seguir los usuarios y responsables de la información para el correcto uso y tratamiento de contraseñas suministradas por Combustibles Líquidos de Colombia S.A. ESP.

Directrices:

Todas las contraseñas de cuentas que den acceso a recursos y servicios de la compañía deberán seguir las siguientes directrices generales:

- Todas las contraseñas de sistema como root, cuentas de administración de aplicaciones, cuentas de administración de servidores, cuentas de administración de correo, administración de equipos y acceso a redes inalámbricas deben ser cambiados al menos una vez cada seis meses.

- Todas las contraseñas de usuario como usuario de equipo, cuentas de email, cuentas de servicios web y cuentas de cliente en aplicaciones deben ser cambiadas al menos una vez cada 60 días.

- Las cuentas de usuario que tengan privilegios de sistema a través de su pertenencia a grupos o por cualquier otro medio, deben tener contraseñas distintas del resto de cuentas mantenidas por dicho usuario en los servicios y recursos.

- Las contraseñas por defecto asociadas a los sistemas o aplicaciones nuevas deberán ser cambiadas antes de poner estos sistemas en producción. También se desactivarán aquellas cuentas “por defecto” que no sean imprescindibles.

7.4.12 Política de seguridad de las comunicaciones

Objetivo: Definir los lineamientos que deben seguirse para asegurar las comunicaciones y sus respectivos mecanismos con el fin de proteger la información de Combustibles Líquidos de Colombia S.A. ESP.

Directrices:

- La gestión de los dispositivos de red debe realizarse si estos los permiten a través de protocolos seguros (Ej. SSH, IPSEC, SSL, etc.).

- Deben utilizarse dominios lógicos (VLAN), firewalls o segmentos físicos para segmentar los diferentes flujos de tráfico que viajen desde y hacia los diferentes sistemas que componen la topología de red de Combustibles Líquidos de Colombia S.A. ESP.

- Debe utilizarse translaciones de red (NAT) para evitar que direcciones internas de Combustibles Líquidos de Colombia S.A. ESP sean expuestas a redes no confiables o públicas.

- Debe garantizarse que cualquier base de datos se encuentre en una zona interna protegida por una DMZ.

- Los sistemas sensibles o críticos deben tener un ambiente informático dedicado (aislado). Es permisible que cohabiten en mismo sistema componentes que hagan parte del sistema principal.

- Todo cambio programado realizado a las reglas de seguridad de red, listas de control de acceso (ACL´s) y/o configuraciones de firewalls, routers e IPS deben ser documentadas.

- Deben establecerse controles para proteger el intercambio de Información que Combustibles Líquidos de Colombia S.A. ESP pueda realizar como parte de sus actividades de Negocio, a través de cualquier canal de comunicación.

- Todo intercambio de información a través de medios electrónicos debe protegerse de acuerdo a su nivel de clasificación.

- Se deben realizar conjuntamente tareas de concienciación y capacitación para que los usuarios sean conscientes sobre los riesgos a los que se pueden ver expuestos cuando se realiza intercambios de información, así como también los controles asociados para la protección de la información.

7.4.13 Política de adquisición, desarrollo y mantenimiento de sistemas

Objetivo: Asegurar la información que se transmite en la adquisición, desarrollo y mantenimiento de sistemas y activos de información de Combustibles Líquidos de Colombia S.A. ESP.

Directrices:

- Especificaciones y requerimientos de controles (automatizados y/o manuales) de seguridad deben siempre ser consideradas cuando se evalúan nuevos productos, software, servicios o en los procesos de desarrollo y/o compras de aplicaciones de negocio.

- Durante los procesos de levantamiento de requerimientos para cualquier sistema o nuevo proyecto, debe contemplarse el diseño e implementación de controles de seguridad.

- Antes de ser adquiridos productos y/o servicios deben establecerse un proceso formal de pruebas, evaluación y adquisición para garantizar que los servicios y/o productos a adquirir cumplan los estándares, políticas y lineamientos de seguridad de la organización.

- En caso que un requerimiento de seguridad no pueda ser satisfecho por el sistema y/o producto a ser adquiridos, debe contemplarse la realización de un análisis de riesgo y la evaluación de controles compensatorios que mitiguen el riesgo de la falta del control principal.

- Cada vez que se requiere un cambio en las aplicaciones y sistemas de información debe seguirse los lineamientos estipulados de controles de cambios.

- En caso de requerirse el uso de datos del ambiente de producción para propósitos de pruebas, debe seleccionarse de manera cuidadosa la porción de datos que ayude a cumplir los objetivos de la prueba y debe establecerse los procedimientos y controles de seguridad para garantizar la confidencialidad e integridad de esta información.

- Para la aprobación de ingreso de un sistema al ambiente de producción debe seguirse el Procedimiento de Control de cambios.

7.4.14 Política de relaciones con los proveedores

- Antes de realizar cualquier tipo de conexión con terceros, debe realizarse un análisis de los riesgos inherentes a la conexión, con el fin de identificar los controles a ser implementados para minimizar el impacto de los mismos.

- Toda conexión nueva hacia redes de terceros debe pasar a través de una revisión de seguridad. Estas revisiones se realizan para garantizar que todos los accesos coincidan con los requerimientos del negocio.

- Debe establecerse acuerdos de intercambio de información y software entre Combustibles Líquidos de Colombia S.A. ESP y cualquier tercero con el cual se requiera realizar este proceso. Estos intercambios en algunos casos son parte del acuerdo contractual firmado entre las partes.

- Los cambios de provisión de conexiones, servicios y/o productos ofrecidos por terceros, incluido políticas de seguridad, procedimientos, controles e información, deben ser administrados de tal forma que se tome en cuenta la criticidad en el negocio, procesos involucrados y revaluación de Riesgos asociados. Los cambios deben ser implementados a través del Procedimiento de Control de Cambios.

7.4.15 Gestión de incidentes de seguridad de la información

- Es responsabilidad de cada colaborador de Combustibles Líquidos de Colombia S.A. ESP, contratista, consultor o tercero, reportar de manera oportuna cualquier evento sospechoso, debilidad o violación de políticas y lineamientos de seguridad a través de los medios establecidos local y corporativamente.

- Debe establecerse procedimiento local de gestión de incidentes que se encuentre alineado al Plan de continuidad de negocio (PCN) de Combustibles Líquidos de Colombia S.A. ESP.

- Cualquier contacto que involucre a las autoridades de investigación y judiciales debe ser escalada al área de relaciones públicas de Combustibles Líquidos de Colombia S.A. ESP, quien establecerá los pasos a seguir.

- Cada vez que se evidencie claramente que Combustibles Líquidos de Colombia S.A. ESP ha sido víctima de un delito informático, una investigación forense debe ser ejecutada. Las investigaciones deben proveer la información suficiente para que la gerencia pueda ejecutar los pasos requeridos para garantizar que el evento no pueda presentarse nuevamente y que las medidas de seguridad asociadas vuelvan a ser restablecidas.

- Todos los incidentes y eventos sospechosos deben ser reportados tan pronto como sea posible a través de los canales internos establecidos por Combustibles Líquidos de Colombia S.A. ESP.

7.5 CONTINUIDAD DEL NEGOCIO

- Debe establecerse las medidas de seguridad necesarias para garantizar que la Información que pudiese almacenarse por requerimientos del negocio se encuentre libre de software malicioso.

- Debe establecerse los controles de seguridad adecuados para evitar la instalación en equipos de cómputo, servidores, equipos de red y comunicaciones de programas o dispositivos que capturen la información de sus clientes y de sus operaciones.

- Debe establecerse los mecanismos necesarios para que el mantenimiento y la instalación o desinstalación de programas o dispositivos en las terminales o equipos de cómputo solo lo pueda realizar personal debidamente autorizado.

- Debe mantenerse ambientes independientes para actividades de pruebas, desarrollo y producción. En todo caso, el desempeño y la seguridad de un ambiente no podrán influir en los demás.

- Debe establecerse procedimientos que permitan verificar que las versiones de los programas del ambiente de producción corresponden a las versiones de programas fuentes catalogadas.

- Debe establecerse los procedimientos y controles para el paso de programas o servicios a producción. El software en operación deberá estar catalogado.

- Debe mantenerse actualizados todos los diagramas de las conexiones y flujos de datos que salen o entran hacia los ambientes de producción.

- Debe mantenerse documentada y actualizada toda la información referente a los parámetros de los sistemas donde operan las aplicaciones en producción, incluido el ambiente de comunicaciones; versión de los programas y aplicativos en uso; soportes de las pruebas realizadas a los sistemas de información; y procedimientos de instalación del software.

- Las pruebas de seguridad como escaneo de vulnerabilidades internas y externas y análisis de redes inalámbricas deben realizarse por lo menos una vez al año.

- Debe tomarse todas las medidas necesarias para remediar las vulnerabilidades detectadas dentro de los análisis. Al final del proceso, debe realizarse un análisis diferencial de vulnerabilidades, comparando el informe actual con respecto al inmediatamente anterior.

- Para todos aquellos activos Core o de alta prioridad por su influencia en la operación de Combustibles Líquidos de Colombia S.A. ESP deben planearse, analizarse, ejecutarse y así mismo auditarse esquemas de redundancia o planes de recuperación ante incidentes o desastres (DRP) que permitan la continuidad del negocio y el menor impacto al flujo de operación de la compañía, tomando como ejemplo aquellos activos como lo son los canales de internet, aplicaciones de facturación, canales de comunicación y demás.

- Todos los funcionarios de la compañía son responsables de los respaldos de la información siguiendo las indicaciones técnicas dictadas por esta política.

- Todos los archivos como documentos, hojas de cálculo, presentaciones, documentos portables (PDF) e imágenes, deben ser cargados o almacenados en la plataforma web Google Docs y preferiblemente trabajados o editados desde ahí.

- Los archivos con extensiones que no pertenezcan al grupo definido como ofimática deben ser almacenados en la herramienta de Google Docs sin ningún tipo de conversión

7.6 CUMPLIMIENTO

Los diferentes aspectos contemplados en esta política son de obligatorio cumplimiento para todos los funcionarios, contratistas y otros colaboradores de Combustibles Líquidos de Colombia. En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, se tomará las acciones disciplinarias y legales correspondientes.

8. PLAN DE CONTINUIDAD

Una vez realizado el proceso de análisis de riesgos donde se identificó los activos de información (aplicaciones, hardware y otros) críticos para el proceso de tecnología, es necesario desarrollar un plan de continuidad de negocio para garantizar que el sistema de gestión de seguridad y los controles definidos, se puedan implementar, con el propósito de minimizar el impacto de la materialización de los riesgos identificados.

El Plan de continuidad del negocio[17], se conforma de un conjunto de directrices y procedimientos plasmados en un documento técnico, para que cada entidad pueda tomar las acciones pertinentes con miras a la recuperación y restablecimiento de los servicios e infraestructuras de TI interrumpidas por situaciones de desastre o emergencias ocurridas en cualquier instante dentro de las organizaciones.

El análisis de impacto del negocio como parte del plan de continuidad del negocio, debe entenderse como un marco conceptual sobre el cual las entidades deben planear integralmente los alcances y objetivos, que permiten proteger la información, en todas sus áreas críticas.

Las entidades deben establecer un análisis de impacto del negocio, que este alineado con el Plan General de Continuidad del Negocio de la Entidad; este debe tener una estrategia de continuidad de TI, que contenga los objetivos globales de la entidad, con respecto a las dimensiones de disponibilidad de datos, infraestructura tecnológica y recurso humano.

Para desarrollar el plan de continuidad del negocio de TI se debe tener en cuenta:

- Diseñar una estrategia de continuidad de los servicios de TI, que tenga como base la reducción del impacto de una interrupción en los servicios críticos de TI del negocio, este debe estar difundido, aprobado y respaldado por los directivos de la entidad.

- Realizar un análisis e identificación de recursos críticos de TI vitales, de esta manera se establece una estrategia que genere prioridades en caso de presentarse una o varias situaciones que causen interrupciones.

- Establecer procedimientos de control de cambio, que permita asegurar que el plan de continuidad de TI, se encuentre actualizado y permita afrontar las amenazas

[17] MINISTERIO DE TECNOLOGÍA, INDUSTRIA Y COMERCIO. Guía impacto de negocio. [en línea], [consultado el 23 de julio de 2016]. Disponible en: http://www.mintic.gov.co/gestionti /615/articles-5482_Guia14_Impacto_Negocio.pdf

que traen consigo las nuevas tendencias tecnológicas sin perder el alcance de los requerimientos de la Entidad.

- Elaborar un plan de pruebas de continuidad de TI, que permita verificar y asegurar que los sistemas de TI, puedan ser recuperados de forma segura y efectiva, atendiendo y corrigiendo errores, que atenten contra la disponibilidad de las operaciones.

- Realizar capacitaciones del plan de continuidad de TI y análisis de impacto del negocio, a los entes o partes involucradas de la organización (Equipo de seguridad de sistemas de información de la entidad), para que conozcan cuáles son sus roles y responsabilidades en caso de incidentes o desastres. Es necesario verificar e incrementar el entrenamiento de acuerdo con los resultados de las pruebas de contingencia generadas dentro de la entidad.

- Tanto el plan de continuidad de TI como el análisis de impacto del negocio deben estar disponibles apropiadamente dentro de la organización y en manos de los responsables de las áreas de TI quienes de forma segura deben garantizar su aplicabilidad en los momentos críticos, a su vez la entidad debe propender por un plan de sensibilización al interior de la misma con el propósito de indicar a todos sus miembros sobre la importancia de contar con un plan de continuidad y de análisis del negocio que van a garantizar el normal funcionamiento de las operaciones regulares en caso de presentarse problemas críticos en los sistemas de información y comunicaciones de la entidad.”

El Plan de Continuidad del Negocio o PCN es una herramienta que permite a Combustibles Líquidos de Colombia y a su proceso de tecnología, mitigar el impacto de un evento o incidente sobre la disponibilidad de los recursos y procesos necesarios para la operación del proceso.

De acuerdo con los controles establecidos en el Ítem 17. Aspectos de la seguridad de la información en la gestión de la continuidad de negocio del Anexo A de la NTC/ISO 27001:2013, se debe incluir la continuidad de seguridad de la información en los sistemas de gestión de continuidad de negocio de la Organización, tal y como se muestra en el cuadro 20.

Cuadro 20. Aspectos de seguridad de la información de la gestión de continuidad de negocio.

Ítem	Aspecto
17.1	Continuidad de seguridad de la información. Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.
17.1.1	Planificación de la continuidad de la seguridad de la información. Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
17.1.2	Implementación de la continuidad de la seguridad de la información. Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información. Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas
17.2	Redundancias Objetivo: Asegurarse de la disponibilidad de instalaciones de procesamiento de información.
17.2.1	Disponibilidad de instalaciones de procesamiento de información. Control: Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

Fuente: WIKIPEDIA. ISO/IEC 27001:2013. [en línea], [consultado el 23 de julio de 2016]. Disponible en: https://es.wikipedia.org/wiki/ISO/IEC_27001

8.1 OBJETIVOS DEL PCN

El plan de continuidad del negocio, tiene como objetivos:

- Proteger ante todo la integridad de las personas y activos de información de la entidad en forma adecuada.

- Lograr la preparación necesaria para responder ante posibles incidentes o amenazas que puedan afectar o interrumpir la operación.

- Garantizar que los Empleados:

- Estén protegidos
- Comprenden su papel

- Saben a dónde ir
- Saben qué hacer
- Saben qué recursos necesitan
- Entienden la secuencia de las tareas críticas

- Minimizar la frecuencia de interrupciones de la operación de los procesos del negocio.

.

- Asegurar una pronta restauración de las operaciones afectadas por el evento que caso la interrupción.

8.2 PRINCIPIOS DEL PCN

El plan de continuidad del negocio, tiene los siguientes principios:

- El plan de continuidad de negocio está orientado a la protección de las personas, así como al restablecimiento oportuno de los procesos, servicios críticos e infraestructura, frente a eventos de interrupción o desastre.

- Todo el personal de la Combustibles Líquidos de Colombia debe estar entrenado y capacitado en los procedimientos definidos y conocer claramente los roles y responsabilidades que le competen en el marco de la continuidad del negocio, mediante labores periódicas de formación, divulgación y prueba de los planes de contingencia del negocio.

- Se debe designar un líder de Plan de Continuidad.

- El proceso de tecnología debe ser recuperado dentro de los márgenes de tiempo requeridos.

- Los procesos y/o servicios que sean desarrollados por terceros contratados deben disponer de planes de continuidad.

- Los planes de contingencia deben mantenerse actualizados, para lo cual se deben desarrollar, probar y de ser necesario mejorar de forma periódica o ante cambios significativos en políticas, personas, proceso, tecnología; siendo necesario que en dicha revisión participen las áreas involucradas.

8.3 ROLES Y RESPONSABILIDADES

A continuación se describen los roles y responsabilidades que deben participar en el plan de continuidad del proceso de TI[18]:

8.3.1 Director de continuidad. El Director de Continuidad es el encargado de dirigir y liderar todas las actividades del plan de continuidad del negocio. Es responsable de declarar la contingencia ante el escenario de interrupción de lugar de trabajo. Sus responsabilidades son:

- Evaluar y aprobar los recursos requeridos para establecer y mantener la estrategia de recuperación y contingencia de la entidad.

- Advertir sobre nuevos riesgos que afectan la continuidad de la operación normal de la entidad y que ponen al descubierto debilidades del plan de continuidad.

- Monitorear los reportes sobre el estado de recuperación o evaluación durante una contingencia.

- Velar por la seguridad del personal que actúa en el área del evento.

- Establecer los objetivos de recuperación y activar el plan de continuidad ante el escenario de interrupción del proceso.

- Velar por la ejecución del debido análisis causa – raíz del evento que ocasionó la contingencia.

8.3.2 Líder de recuperación tecnológica. Es la persona encargada de liderar la recuperación tecnológica, basados en las estrategias de continuidad implementadas. Es el contacto directo entre la Dirección de Tecnología y el director de continuidad; además, apoya las decisiones tomadas por el Director de Continuidad durante la declaración y activación de la contingencia. Sus responsabilidades son:

- Liderar la recuperación tecnológica, basados en las estrategias de continuidad implementadas.

---

[18] ICETEX. Manuales de continuidad de roles y responsabilidades. . [en línea], [consultado el 23 de julio de 2016]. Disponible en: https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manual_continuidad

- Identificar los posibles riesgos de aspectos tecnológicos que afectan la continuidad de la operación normal de la entidad y que ponen al descubierto debilidades del plan de continuidad.

- Colaborar en la comunicación a los proveedores de los temas o servicios de su competencia, sobre el estado de contingencia en que se encuentra la Entidad, esto previa decisión y autorización del Director de Continuidad, mediante comunicado elaborado en conjunto con la Oficina Asesora de Comunicaciones.

8.3.3 Responsable de tareas de apoyo. Sus responsabilidades son:

- Realizar las actividades que le sean asignadas durante la declaración de contingencia.

- Advertir sobre riesgos que puedan afectar la continuidad en la prestación del servicio o la funcionalidad del plan.

Cada área cuenta con un Líder de PCN, quien tiene las siguientes responsabilidades en la administración del plan de continuidad sobre los procesos y/o procedimientos a cargo:

- Actuar como punto focal del área para todos los asuntos de continuidad del negocio.

- Cumplir con las actividades y fechas establecidas del cronograma de PCN.

- Mantener informados a todos los colaboradores de sus respectivas áreas, los planes de contingencia que les compete.

- Asegurar la aplicación correcta de los PCN al interior del área.

8.4 ANÁLISIS DE IMPACTO DE NEGOCIO

8.4.1 Evaluación de impacto. Teniendo en cuenta los elementos operacionales de la organización, se requiere evaluar el nivel de impacto de una interrupción dentro de la entidad. El impacto operacional permite evaluar el nivel negativo de una interrupción en varios aspectos de las operaciones del negocio; el impacto se puede medir utilizando un esquema de valoración, con los siguientes niveles: A, B o C.

- Nivel A: La operación es crítica para el negocio. Una operación es crítica cuando al no contar con ésta, la función del negocio no puede realizarse.

- Nivel B: La operación es una parte integral del negocio, sin ésta el negocio no podría operar normalmente, pero la función no es crítica.

- Nivel C: La operación no es una parte integral del negocio.

El cuadro 21 muestra los niveles de criticidad, que contempla un sistema de tolerancia a fallas por horas, cuya propiedad permite que un sistema pueda seguir operando normalmente a pesar de que una falla haya ocurrido en alguno de los componentes del sistema; por lo tanto la tolerancia a fallas es muy importante en aquellos sistemas que deben funcionar todo el tiempo.[19]

Cuadro 21. Evaluación de Impacto

Función de negocio	Proceso (Servicio)	Tolerancia a fallas (Horas)	Nivel de criticidad
Aplicaciones Core	Sistemas o Aplicaciones Core del Negocio	3	B
Blade Center	Arreglo de servidores que contiene servidor de demonio, servidor de datos y servidor de aplicaciones no core	3	B
Copias de seguridad	Copias de seguridad y backup de diferentes dispositivos	3	B
Data Center	Servicio de Centro de datos de la Entidad	1	A
Bases de Datos	Bases de datos de las aplicaciones core del Negocio	1	A
Canales de internet y de comunicaciones	Acceso Local a Internet	4	C
Firewall	Seguridad de la Información.	1	A
Recurso Humano	Internos	3	C
Fuente: Autores			

[19] MINISTERIO DE TECNOLOGÍA, INDUSTRIA Y COMERCIO. Op. Cit, p. 156

El proceso de Tecnología, es un proceso de apoyo, el cual tiene como objetivo prestar el servicio de administración y soporte de la infraestructura tecnológica y sus plataformas, para asegurar el funcionamiento operativo de la compañía.

8.4.2 Escenarios de falla. A partir de las causas de los posibles riesgos identificados se referencian las acciones a seguir en caso que las mismas se presenten. Estas se pueden unificar en el cuadro 22:

Cuadro 22. Escenarios de falla

Categoría	Escenario	Descripción de Impacto
Red Eléctrica	Fallas en el fluido eléctrico red normal (no regulada)	Fallas del servicio eléctrico de la entidad que afecta equipos eléctricos normales.
	Fallas en el Fluido Eléctrico red regulada	Fallas en los servicios de Tecnología de Información.
Red Datos, Internet y Seguridad	Problemas dispositivos Red: Falla Total	Falla general de los servicios de TI de todos los componentes por ausencia en las comunicaciones
	Problemas en los Dispositivos Seguridad: Falla Total	Falla general de los servicios de TI de todos los componentes que tiene que ver con elementos de seguridad de TI (Elementos de Hardware, Software) y ausencia de políticas y controles de TI.
	Ausencia servicio del canal de Internet Última Milla	Falla general de los servicios de TI de todos los componentes involucrados en la conexión de última milla por ausencia en la comunicación.
Hardware distribuido	Problema de Hardware de Servidores: Falla Total	Falla total de los servicios de los sistemas de información que usan la plataforma de servidores.
	Problemas Hardware de Servidores	Falla de los servicios de los sistemas de información que usan la plataforma de servidores.
Aplicaciones infraestructura distribuida	Problemas Capa de Aplicaciones	Falla o degradación del servicio prestado en el sistema de información afectado por problemas en las aplicaciones.
	Problemas Capa Media	Falla o degradación de la aplicación soportada por las herramientas de software y el sistema de almacenamiento masivo de datos – SAN, por tanto se puede presentar degradación o ausencia del servicio prestado por sistema de información afectado por problemas de la capa media.

Cuadro 22. (Continuación)

	Problemas Capa de Bases de Datos	Falla o degradación de las aplicaciones soportadas por las herramientas y motores de Base de Datos, por tanto se puede presentar degradación o ausencia del servicio prestado por los sistemas de información afectados por problemas de la capa de base de datos.
Recurso Humano	Errores humanos en operación	Contempla desde la degradación de un servicio hasta la pérdida del mismo, como también la ejecución de procedimientos de manera errada que de cómo resultado la pérdida del servicio de uno o todos los sistemas de información del proyecto
Fuente: MINISTERIO DE TECNOLOGÍA, INDUSTRIA Y COMERCIO. Guía impacto de negocio. [en línea], [consultado el 23 de julio de 2016]. Disponible en; http://www.mintic. gov.co/gestionti/615/articles-5482_Guia14_Impacto_Negocio.pdf		

8.4.3 Identificación de recursos. Las diferentes actividades contempladas en la función crítica del negocio deben considerarse de vital importancia cuando apoyan los procesos críticos del negocio. Por lo tanto es clave en este punto, la identificación de recursos críticos de sistemas de tecnología de Información que permitan tomas acciones para medir el impacto del negocio de las Entidades[20]. La cuadro 23 identifica los recursos críticos de sistemas de tecnologías de Información:

Cuadro 23. Recursos críticos

Función de Negocio	Proceso (Servicio)	Escenario de Falla
Aplicaciones Core	Sistemas o Aplicaciones Core del Negocio	Problemas Capa de Aplicaciones
Blade Center	Arreglo de servidores	Problemas Hardware de Servidores
Data Center	Servicio de Centro de datos de la Entidad	Fallas en el fluido eléctrico red normal (no regulada)
Bases de Datos	Bases de datos de las aplicaciones core del Negocio	Problemas Capa de Bases de Datos
Canales de internet y de comunicaciones	Acceso Local a Internet	Problemas dispositivos Red: Falla Total
Firewall	Seguridad de la Información.	Problemas en los Dispositivos Seguridad: Falla Total
Fuente: Autores		

[20] WIKIPEDIA. Op. Cit. p. 115

8.5 DISEÑO DE ESTRATEGIAS

El objetivo del diseño de estrategias de continuidad de negocio, es evaluar y seleccionar estrategias de continuidad que más se adecuen a los procesos críticos del negocio. Las estrategias de continuidad se diseñaron considerando los tiempos objetivos de recuperación:

- Instalaciones físicas: El proceso de tecnología, cuenta con una sala de cómputo, el cual funcionaría como puesto de trabajo, en caso de ser requerido. Sumado a ello, dicha sede se encuentra en las afueras de la ciudad, lo que no implicaría traumatismos al momento de que los usuarios necesiten acceder a los servicios con una infraestructura espejo con la topología semejante a la de la sede principal tipo cloud.

- Hardware: se cuenta con equipos de cómputo con las características necesarias para funcionar, atendiendo a las necesidades de los procesos de la organización, en su capacidad total operativa.

- Software: dado que el software es requerido para el desarrollo de los procesos, el mismo debe contar con una copia de seguridad, debidamente almacenada, para que en caso de que ocurra un siniestro.

- Redes de comunicación y servicios: Combustibles Líquidos de Colombia cuenta con una red de comunicaciones capaz de soportar el flujo de comunicaciones y de datos de los procesos.

- Personas: con el fin de minimizar al máximo la interrupción de los procesos en lo que respecta al personal, se procederá a capacitar a cada uno de los funcionarios, con el fin de que cada uno conozca y desarrolle sin limitantes los puestos de trabajo o subprocesos propios de cada una.

9. CONCLUSIONES

Se diseñó un Sistema de Seguridad de la Información para Combustibles Líquidos de Colombia S.A. ESP, que permitió identificar los riesgos a los que se ve expuesta la compañía en conjunto con la propuesta del respectivo plan de tratamiento a través de la valoración de sus activos de información y de los lineamientos que ofrece el estándar ISO/IEC 27001:2013.

Se propuso a Combustibles Líquidos de Colombia S.A. ESP una política de seguridad de la información que permitirá fortalecer y poner en funcionamiento el sistema de gestión de seguridad de la información diseñado para la organización.

El Sistema de Gestión de Seguridad de la Información es un proceso sistemático, con el cual Combustibles Líquidos de Colombia, va a lograr la implantación de políticas, procedimientos, y controles, para minimizar cualquier riesgo al que pueda estar expuesto sus activos de información.

El Diseño de este marco de trabajo para Combustibles Líquidos de Colombia, va permitir que los demás procesos de la organización, puedan operar en condiciones seguras. De igual forma los funcionarios de la entidad, podrán reconocer la seguridad como un pilar para el desarrollo de los procesos.

10. RECOMENDACIONES

Se recomienda continuar con la implementación y madurez del sistema de gestión de la seguridad de la información en Combustibles Líquidos de Colombia, para lo cual se debe realizar el proceso de identificar activos en los demás procesos de la Organización. Se debe identificar los posibles Riesgos de los activos identificados, y aplicar las demás etapas sugeridas en el diseño del SGSI para la organización.

Se debe crear una campaña de sensibilización y entrenamiento de todos los funcionarios de todos los procesos que hacen parte de la cadena de valor de Combustibles Líquidos, para que identifiquen y den tratamiento adecuado a los posibles riesgos a los que pueda estar expuesta la información.

Se debe desarrollar ejercicios de análisis de vulnerabilidades sobre los activos de información de Combustibles Líquidos, con el fin de identificar y tratar las posibles vulnerabilidades. De igual forma se recomienda, implementar monitoreo sobre la red, con el propósito de identificar anomalías, virus y problemas en la red.

El SGSI se debe auditar y se debe revisar por la Dirección una vez se tenga un grado de madurez o un grado de implementación más profundo sobre los diferentes procesos incluidos en el alcance, para lo cual se recomienda realizar una revisión interna y luego una revisión de un tercero, con el propósito de verificar la efectividad del SGSI.

BIBLIOGRAFÍA

BLOG DE BITCOMPANY. Los beneficios que ofrecen el Project Management, COBIT y normas ISO a las organizaciones que lo implementan. [En línea], [consultado el 25 de abril de 2016]. Disponible en: www.**bitcompany**.biz/.

BRYDEN, Alan, COPANT Seminar on Security Standards, La Paz, 25 de abril de 2006. [En línea], [consultado el 25 de abril de 2016]. Disponible en: http://www.iso.org/iso/livelinkgetfile? llNodeId=21657&llVolId=-2000

CARO Y CUERVO. ¿Qué es política de seguridad? [En línea], [consultado el 25 de abril de 2016]. [En línea], [consultado el 25 de abril de 2016]. Disponible en: www.caroycuervo.gov.co/ sites/.../POLÍTICA% 20DE%20 SEGURIDAD% 20ICC_0.pd

DEFINICIONES ABC. ¿Qué es amenaza? [En línea], [consultado el 25 de abril de 2016]. Disponible en: www.definicionabc.com › General

DEFINICIONES MX. ¿Qué es Prevención de riesgos? [En línea], [consultado el 25 de abril de 2016]. Disponible en: definicion.de/prevención-de-riesgos/

ESCUELA DE ADMINISTRACIÓN. Mapa de riesgos. [En línea], [consultado el 3 de agosto de 2016]. Disponible en: http://www.eafit.edu.co/escuelas/ administracion/consultorio-contable/ Documents / Nota %20de%20clase%2016 %20Mapa%20de%20Riesgos.pdf

ESCUELA DE ADMINISTRACIÓN, FINANZAS Y TECNOLOGÍA. ¿Qué son medidas de tratamiento? [En línea], [consultado el 25 de abril de 2016]. Disponible en: www.eafit.edu.co/.../Nota%20de%20Clase%2010%20 Medidas% 20de%20Tratamiento

ICETEX. Manuales de continuidad de roles y responsabilidades. [en línea], [consultado el 23 de julio de 2016]. Disponible en: https://www.icetex.gov.co/ dnnpro5/Portals/0/ Documentos/La%20Institucion/manuales/Manual_continuidad

INSTITUTO URUGUAYO DE NORMAS TÉCNICAS. Normalización: ISO 27000. [En línea], [consultado el 25 de abril de 2016]. Disponible en: http://www.unit.org. uy/vista/html/_img/normalizacion/ sist_27000_ que.png

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Norma Técnica Colombiana NTC 5411-1. Bogotá: ICONTEC, 2005

INSTITUTO ESPAÑOL DE ANALISTAS. ¿Qué es control? [En línea], [consultado el 25 de abril de 2016]. Disponible en: ieaf.es/new/lideres-de.../control-y...riesgos.../1561-que-es-el-control-de-riesgos.html

ISO/IEC 27001. ISO 27001 - Sistema de gestión de la seguridad de la información: requisitos. [En línea], [consultado el 25 de abril de 2016]. Disponible en: www.gesconsultor.com/iso-27001.html

ISO/IEC. Norma ISO/IEC 27001:2013, 6.1.2 Evaluación de riesgos de la seguridad de la información. Op. Cit. p. 25

ISOTOOLS COLOMBIA. El plan de gestión de riesgos según la norma ISO 27001- [En línea], [consultado el 3 de agosto de 2016]. Disponible en: https://www.isotools.org/2013/12/26/ el-plan-de-gestion-de-riesgos-segun-la-norma-iso-27001/

JURAN, J. (2012). Total igualdad de producto por igualdad de proceso. [En línea], [consultado el 25 de abril de 2016]. Disponible en: http://www.totalqualidade.com.br/2012/09/

MINISTERIO DE TECNOLOGÍAS DE INFORMACIÓN. Glosario. [En línea], [consultado el 28 de septiembre de 2016]. Disponible en: www.mintic.gov.co/gestionti/615/articles-6099_recurso_2.docx › General

MINISTERIO DE TECNOLOGÍA, INDUSTRIA Y COMERCIO. Guía impacto de negocio. [En línea], [consultado el 23 de julio de 2016]. Disponible en: http://www.mintic.gov.co/gestionti /615/articles-5482_Guia14_Impacto_Negocio.pdf

_____. Definición de Probabilidad e Impacto, [En línea], [consultado el 3 de agosto de 2016]. Disponible en: http://www.mintic.gov.co/gestionti/615/articles-5482_Gestion_Riesgo.pdf

MORENO, Fernando. ISO 27003 (SGSI) Ayuda y guía para implementar un SGSI. CISM 2015. . [En línea], [consultado el 25 de abril de 2016]. Disponible en: https:// es.scribd.com/doc/.../ISO-27003-SGSI-Ayuda-y-Guia-Para-Implementar-

SUPERINTENDENCIA FINANCIERA. Norma ISO/IEC 27001:2013, 6.1.2 Evaluación de riesgos de la seguridad de la información. [En línea], [consultado el 3 de agosto de 2016]. Disponible en: https://www. superfinanciera.gov.co/ SFCant/NormativaFinanciera/Archivos/ance048_06.rtf

WELIVE SECURITY. Análisis de riesgos. [En línea], [consultado el 25 de abril de 2016]. Disponible en: www.welivesecurity.com/la-es/2012/08/16/en-que-consiste-analisis-riesgos/

_____. ¿Qué es declaración de aplicabilidad?. [En línea], [consultado el 25 de abril de 2016]. Disponible en: www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa/

WIKIPEDIA. ISO/IEC 27001:2013. [en línea], [consultado el 23 de julio de 2016]. Disponible en: https://es.wikipedia.org/wiki/**ISO/IEC**_27001

WORDPRESS. Ciclo pdca en 27001-2013. [En línea], [consultado el 25 de abril de 2016]. Disponible en: https://trabajoscun.files.wordpress.com/2014/ 03/ciclo-pdca-en-27001-2013

_____. ¿Qué es un activo de información?. [En línea], [consultado el 25 de abril de 2016]. Disponible en: https://camiloangel.wordpress.com/2010/09/03/¿que-es-un-activo-de-informacion.

ANEXOS

Anexo A. Solicitud de Aval para Proyecto

Ruben Dario Espitia Manrique <respitia@clcgas.com.co>

Solicitud de Aval para proyecto

2 mensajes

Ruben Dario Espitia Manrique <respitia@clcgas.com.co> 18 de junio de 2015, 9:25
Para: Willinton Ayala Mosquera <wayala@clcgas.com.co>
Cc: Carlos Leonidas Alcala Payares <tecnologiaclc@clcgas.com.co>, Patricia Mahecha <pmahecha@clcgas.com.co>, Alejandro Alvarez <alejandro.alvareza@gmail.com>, NICOLAS CANTOR <nicolascantor.sanchez@gmail.com>

Muy buen día Ingeniero,

El presente correo tiene como objetivo obtener su Aval y consentimiento para aplicar en CLC el proyecto de grado de la Especialización en seguridad informática (actualmente en curso), ya que la idea es entregarle a la compañía un valor agregado en cuanto a temas de seguridad se trata, así que como proyecto tenemos con 2 compañeros de la Universidad Piloto de Colombia la implementacion de un sistema de gestión de la seguridad de la información o SGSI teniendo como referencia el estándar ISO 27001:2013, aplicando de tal manera nuestro conocimiento y experiencia en todo este proceso dentro de CLC.

También me parecería importante que nos regalara una cita en donde podamos explicarle a detalle el respectivo proceso de implementación y el alcance del mismo, junto con las personas involucradas, tales como lo son, el Ing. Alejandro Alvarez, Ing. Nicolas Cantor, Ing. Carlos Alcala como nuestro director de tecnologia, Ing. Patricia Mahecha como nuestra directora de proyectos y usted como la alta gerencia.

De ante mano agradecemos su atención y quedamos muy atentos a sus valiosos comentarios.
--

Cordialmente,

Ruben Dario Espitia Manrique.
Ingeniero Electronico y de telecomunicaciones.
Coordinador de Tecnologia.
Combustibles Liquidos de Colombia SA ESP
3138887654

Willinton Ayala Mosquera <wayala@clcgas.com.co> 18 de junio de 2015, 9:27
Para: Ruben Dario Espitia Manrique <respitia@clcgas.com.co>
Cc: Carlos Leonidas Alcala Payares <tecnologiaclc@clcgas.com.co>, Patricia Mahecha <pmahecha@clcgas.com.co>, Alejandro Alvarez <alejandro.alvareza@gmail.com>, NICOLAS CANTOR <nicolascantor.sanchez@gmail.com>

Por mi no hay problema. Gracias.
[El texto citado está oculto]

Anexo B. Política de uso de recurso informático

CLC	**POLITICA DE RECURSOS INFORMATICOS**	gaz

1. **Objetivos:** Definir las políticas, disposiciones y procedimientos para la administración, el uso adecuado y seguro de los recursos tecnológicos y de servicio de Combustibles Líquidos de Colombia S.A.E.S.P, y garantizar la operación de la compañía.

2. **Alcance:** Este documento aplica para todos los sistemas, versiones y plataformas instaladas en Combustibles Líquidos de Colombia S.A.E.S.P y debe ser conocido e implementado por todos los usuarios de la compañía.

3. **Responsable:** Todos los usuarios de la compañía.

4. **Definiciones:**

   Recursos tecnológicos y de servicio: Conjunto de elementos disponibles para resolver una necesidad de la compañía en hardware y software.
   Acceso: Manera más común de conceder o de restringir el ingreso a la información, o acceso a los equipos; que para el caso está dado por el uso de contraseñas y cuentas.

5. **Documentos soporte:**
   R5-P001 Gestión de Recursos Tecnológicos.
   R5-F001 Formato Solicitud de recursos tecnológicos.

6. **Disposiciones Generales:** Las disposiciones definidas tienen carácter obligatorio y su adopción e implementación está a cargo de los Directores de todas las áreas de la organización.
   Es responsabilidad de la Dirección de Tecnología en cabeza del Director verificar el cumplimiento de estas políticas y el permanente monitoreo y auditoria usando las herramientas de cada sistema.
   Todos los usuarios son responsables de cumplir las disposiciones contenidas en este documento.

7. **Descripción de las actividades:**

   7.1 Políticas de Uso de los Recursos Tecnológicos y de Servicio:
   Todo acceso y uso de los recursos tecnológicos de Combustibles Líquidos de Colombia S.A.E.S.P, debe regirse por las normas de disponibilidad, confiabilidad e integridad de la información definidas por la Dirección de Tecnología.

   • Toda la información contenida en los equipos informáticos es de propiedad de Combustibles Líquidos de Colombia S.A.E.S.P y por lo tanto puede ser auditada, monitoreada, modificada y/o eliminada de acuerdo con las políticas establecidas por la Dirección de Tecnología.

   • Toda la información contenida en los equipos informáticos es propiedad de Combustibles Líquidos de Colombia S.A.E.S.P y por lo tanto es de carácter confidencial. Ninguna parte de su contenido puede ser usada, copiada ni divulgada sin autorización de Combustibles Líquidos de Colombia S.A.E.S.P.

   • Los recursos tecnológicos suministrados son para uso exclusivo en las actividades de Combustibles Líquidos de Colombia S.A.E.S.P.

   - El uso de Software no autorizado o adquirido ilegalmente, es considerado como PIRATA y por tanto una violación a los derechos de autor.

Anexo B. (Continuación)

• El no cumplimiento de las políticas y disposiciones contenidas en este documento y las adicionales que consideren las directivas de Combustibles Líquidos de Colombia S.A.E.S.P, derivara sanciones de tipo laboral, teniendo en cuenta parámetros como la gravedad de la falta y el impacto en el negocio.

7.1.1 Claves de acceso

7.2.1 El jefe inmediato debe diligenciar el formato **R5-F001** Formato Solicitud de recursos tecnológicos, en el que solicita se le asigne a la persona que ingresa a la compañía, acceso a la red y a los recursos tecnológicos, y los funcionarios de la dirección de tecnología mediante el procedimiento **R5-P001** Gestión de Recursos Tecnológicos efectúa el alistamiento y entrega del recurso informático, se le crean y conceden las cuentas o acceso a los diferentes sistemas y equipos de la compañía, el mantenimiento apropiado de estas cuentas , así como del password de acceso es esencial para garantizar la seguridad de la propiedad intelectual de Combustibles Líquidos de Colombia S.A.E.S.P en los sistemas de información. Por lo anterior:

- Es responsabilidad de cada usuario proteger el nombre de usuario y las contraseñas de acceso asignadas.
- Una contraseña se considera información clasificada, es decir que es de uso personal e intransferible.
- Ningún usuario de los sistemas de información puede acceder al sistema con claves ajenas. En caso de pérdida de información el responsable es aquel que entregó sus claves de acceso.
- No se deben enviar por correo electrónico las credenciales de acceso, como son el nombre de usuario o la contraseña.
- No entregue su contraseña a compañeros de trabajo, Gerente y Directores de Área.
- El usuario es responsable de cambiar la contraseña periódicamente o en caso que detecte fallos en la seguridad.
- En el caso en que se detecte a un empleado accediendo a un sistema de información con claves ajenas, estas serán bloqueadas inmediatamente y se notificará al Gerente o Director del área, para que tome las medidas necesarias.

7.2.2 Correo electrónico

- La cuenta de correo electrónico debe ser usada únicamente para fines laborales o para aquellas funciones asignadas por Combustibles Líquidos de Colombia S.A.E.S.P
- No está permitido el uso de las cuentas de correo electrónico asignadas, para fines personales o ajenos al carácter laboral para que fueron creadas; además no está autorizada la configuración de cuentas diferentes al dominio @clcgas.com.co
- Los archivos que se envíen no pueden superar un tamaño de 20 MB y cuando están cerca de este tamaño su envío se debe realizar en horas de poco tráfico.
- Todos los archivos enviados por este medio deben esta comprimidos (".ZIP) ya que este procedimiento agilizará la entrega y evitara fallos o retrasos del sistema.
- No se permite el envío de archivos ejecutables (Nombre_del_archivo.**EXE**), de procesamiento por lotes (Nombre_del_archivo.**BAT**) o de comandos (Nombre_del_archivo.**COM**), ya que la mayoría de los sistemas de antivirus impiden recibirlos por el destinatario.

Anexo B. (Continuación)

	POLITICA DE RECURSOS INFORMATICOS	

7.2.3 Internet

- El servicio de Internet debe ser usado únicamente para fines laborales o para aquellas funciones asignadas por Combustibles Líquidos de Colombia S.A.E.S.P
- Queda restringido el uso de aplicaciones de tipo P2P (Peer-to-Peer) en las que se pueden intercambiar cualquier tipo de archivos. Este tipo de aplicaciones son potencialmente peligrosas ya que tienen fallos de seguridad y facilitan la distribución de archivos con virus. De igual manera queda restringida la instalación de software Shareware, Freeware o Trialware sin aprobación de La Dirección de Tecnología.
- Es responsabilidad del usuario toda la información que manipule en Internet y se le hace responsable por cualquier operación irregular en la que este incurriera.
- No se permite el ingreso a sistemas de Chat personales y suscripciones a correos masivos en las que se suministra una cuenta de correo de Combustibles Líquidos de Colombia S.A.E.S.P.
- Está prohibido utilizar software que permita violar las reglas de seguridad aplicadas por el Firewall o sistemas de seguridad.
- No se permite la visualización de contenido que incite a las apuestas, la intolerancia, la pornografía o de cualquier material que atente contra la integridad del ser humano.

Acuerdo

Declaro haber leído y comprendido la presente Política de Utilización de Recursos Informáticos y de servicio, en prueba de lo cual firmo mi conformidad con la misma.

Firma: _____

Fecha: _____

8. Relación de novedades y cambios

Fecha	Versión	Creado por:	Revisado por:	Aprobado por:	Modificación del documento
04-10-12	1	Pedro Slatova/Coord. Tecnología	Sarely López/Calidad	María Cortes/Gerente E	Elaboración Inicial
15-07-13	2	O. Hernández / Dir. Calidad	F. Otalora/Dir. Tecnología	W. Ayala	Actualización Políticas

Anexo C. Procedimiento creación hojas de vida de equipos de cómputo

	PROCEDIMIENTO CREACION HOJAS DE EQUIPOS DE COMPUTO CLC	

5. RELACIÓN DE NOVEDADES Y CAMBIOS

Fecha	Versión	Elaborado por:	Revisado por:	Aprobado por:	Modificación del documento
27/02/2014	1	Rubén Darío Espitia	F. Otalora / Dir Tecnología	F. Otalora / Dir Tecnología	Elaboración inicial
27/07/2016	2	O. Hernandez/Dir. Calidad	C. Alcalá / Dir Tecnología	C. Alcalá / Dir Tecnología	Actualización (definiciones)

Anexo D. Seguimiento a recursos tecnológicos

	**SEGUIMIENTO A RECURSOS TECNOLOGICOS**	

1. **Objetivos:** Establecer y mantener un inventario de recursos tecnológicos (servidores, almacenamiento, PC's, dispositivos de networking, productos de software, aplicaciones de negocio y todo objeto administrable por el área de IT) así como servir de base para el seguimiento de cambios a componentes.

2. **Alcance:** Se encuentra dirigido a los administradores de los activos de hardware y software de IT.

3. **Responsable:** Líder: Director IT

4. **Documentos Soporte:**

R5-F006 Planilla De Inventario It
R5-I003 Seguimiento de Software instalado.
R5-F007 Seguimiento de Software

5. **Disposiciones Generales:** La Gestión de Configuraciones constituye una mejor práctica con respecto a la identificación única, almacenamiento controlado, control de cambios e inventario perpetuo de los componentes de IT (Hardware/Software). La información será administrada en SalesForce y debe servir y ser utilizada para:

   - Planificar el impacto de futuros cambios, ya sea de infraestructura o aplicaciones.

   La instalación de software legal permite ventajas como utilizar componentes extras, paquetes de actualización y soporte técnico, así como evitar que la compañía incurra en problemas legales. Con este propósito la Dirección IT incluye dentro de sus herramientas de gestión OCS Inventory, un aplicativo que permite la centralización de información referente al software instalado en cada equipo de cómputo. La administración del Software OCS Inventory la realiza única y exclusivamente área de IT.

Anexo D. (Continuación)

	SEGUIMIENTO A RECURSOS TECNOLOGICOS	

6. Descripción de la Actividad:

	Responsable
6.1 La información encontrada en SalesForce debe contar con las siguientes características: • Una identificación única y consistente de cada ítem de IT. • Información de estado de cada ítem (Disponible, en uso, en configuración, inactivo).	Área IT
6.2 En forma regular, se debe revisar el inventario completo de activos físicos y lógicos para asegurar que los ítems configurados se encuentren correctamente parametrizados, actualizados y controlados. Para el caso de los activos una vez por año o por solicitud de la gerencia en caso de ser necesario, generando el informe **R5-F006Planilla De Inventario activos físicos IT** que incluye los siguientes campos y es generado desde Salesforce automáticamente: • Código de inventario • Serial del equipo • Responsable del equipo • Marca • Referencia • Estado • Ubicación • Fecha de Revisión • Observaciones Una vez generado el informe se realizará la comparación contra el inventario físico confirmando la información consignada en el reporte y generando los cambios necesarios para mantener completamente actualizado el parque informático en la plataforma SalesForce. 6.3 En el caso de los productos de software se realizara una revisión trimestral utilizando la herramienta OSC Inventory de acuerdo al instructivo **R5-I003 Seguimiento de Software instalado**. Para el inventario de software se realizarán las siguientes actividades: 1. Revisión de los todos los productos de software instalados.	administrados por IT el inventario físico se realiza Área IT

Anexo D. (Continuación)

	SEGUIMIENTO A RECURSOS TECNOLOGICOS	

2. De llegar a existir instalado software no permitido en el equipo en seguimiento, se procederá a registrar la novedad en el formato **R5-F007 Seguimiento de Software**, donde se llevará la información correspondiente al responsable del equipo, nombre del equipo, fecha de instalación del software y nombre del mismo. En caso de no encontrar evidencia se debe dejar un registro indicando que la revisión fue realizada y que no se encontraron hallazgos relevantes. 3. Después de realizado el registro, se procederá a desinstalar el software no permitido y se notificará mediante un mail al Director de IT que la revisión fue realizada y las medidas correctivas aplicadas. 4. Cuando la persona reincide por segunda vez con la instalación de software no permitido, se notificará al jefe inmediato, a la Dirección Administrativa y a jefe de Gestión Humana para que se tomen las medidas correctivas del caso, debido al incumplimiento de las políticas establecidas por parte del usuario.	
6.4 De registrarse faltantes injustificados en activos físicos se deberá confeccionar y elevar un informe al Director IT con el detalle completo del faltante.	Área IT

7. Relación de novedades y cambios

Fecha	Versión	Creado por:	Revisado por:	Aprobado por:	Modificación del documento
04-10-12	1	Pedro Siatova/ Coord. Tecnologia	Sarely López/Calidad	María Cortes/Gerente E	Elaboración inicial

Anexo E. Procedimiento de atención mesa de ayuda

	IT **ATENCION AL USUARIO IT**	

1. **Objetivos:** Describir el procedimiento de atención a los usuarios, ofrecido por la mesa de ayuda de la Dirección de IT para garantizar la protección de la información y solución de fallos.

2. **Alcance:** Este procedimiento es aplicable a todas las áreas de la compañía que realizan solicitudes tales como equipos de telefonía, equipos de cómputo, soporte técnico y cualquier otro elemento físico que tenga un impacto sobre la productividad de algún área, que van dirigidas hacia la Dirección de IT.

3. **Responsable:** Director IT - Coordinador IT

4. **Documentos Soporte:**
   R5-I002 Registro de casos mesa de ayuda

5. **Definiciones:**

   Numero de caso: Es un número asignado al requerimiento del usuario por la mesa de ayuda para su atención y control.
   Requerimientos o tipo de solicitud: Pregunta que se hace a la mesa de ayuda con el propósito de dar solución a un problema.
   Usuario: Es la persona, organización u otra entidad que depende de los servicios de un computador o sistema de información para obtener un resultado deseado.

6. **Políticas de Atención a los usuarios:**

   Para garantizar que la atención a los usuarios sea lo más efectiva posible, es indispensable el registro de todos los requerimientos independiente de origen o tipo de solicitud, bien sea infraestructura, software, entrenamiento etc.

   Dicha solicitud se realizará mediante un correo electrónico, telefónicamente o a través del registro formal en la herramienta del CRM a través del enlace http://clcgas.force.com/helpdesk, como lo indica el instructivo **R5-I002** Registro de casos mesa de ayuda. Una vez creado el caso por el usuario llegará una notificación automática vía correo electrónico indicando la apertura del caso.

   Puesto que no todas las solicitudes tienen el mismo impacto en las operaciones de la empresa, la importancia del caso dependerá del tipo de problema registrado.

- **Alto** → Cualquier evento que no es parte de la operación estándar de un servicio corporativo y que causa, o puede causar, una interrupción de un servicio o una reducción

Anexo E. (Continuación)

en la calidad del mismo, requiere de solución inmediata ya que el impacto en el negocio puede ser relevante.

- **Medio→** El sistema o aplicación, opera con funcionalidades limitadas, pero existen alternativas paralelas, los servicios corporativos no se ven afectados a corto plazo pero requieren atención.

- **Bajo→** No requiere de atención inmediata ya que existen elementos o aplicaciones que pueden suplir temporalmente el daño sin afectar el desempeño o rendimiento del usuario.

- **Notificación apertura del caso**

Se notifica automáticamente al usuario mediante un mail una vez crea el caso interno.

- **Notificación de avance de la solicitud**

El Coordinador de IT que está atendiendo un caso, mantendrá informado al usuario sobre los avances que se presenten, actualizando el caso interno en Salesforce.

Retención de Información

Debe medirse la satisfacción y la percepción que el cliente tiene sobre los servicios de IT, para ello, se ejecutarán las siguientes actividades.

1) **Encuesta de Servicio**: Cada trimestre se llevará a cabo la encuesta de servicio, la cual debe ser diligenciada por todos los clientes de la Dirección IT. El resultado de esta encuesta permitirá determinar necesidades de nuestros clientes internos y opciones de mejora sobre el servicio ofrecido por la Dirección de IT. Esta encuesta es realizada vía web a través de la plataforma de Google Apps por los usuarios y la Dirección IT es la encargada de consolidar los resultados.

   Agenda IT - Planeación por área: El Director IT se reunirá con las áreas usuarias que soliciten apoyo de tecnología para el desarrollo de sus proyectos. Estas reuniones deben servir para: interiorizarse de nuevas necesidades, cambiar prioridades, consensuar fechas de necesidad y entrega; y toda otra información que permita por un lado a IT planificar y organizar su trabajo, y por otra al usuario comunicar y priorizar sus necesidades y estar informado del avance de las soluciones que ha solicitado. Los avances de los proyectos deben ser registrados en el R5-F00X Acta de Reunión IT.

Anexo E. (Continuación)

CLC	IT ATENCION AL USUARIO IT	gaz

7. Descripción de la actividad:

ACTIVIDADES	RESPONSABLES
7.1 Recepción de requerimientos Se recibe el caso interno, llamada, correo electrónico o documento formal de solicitud de los usuarios, el procedimiento a seguir se basa en las actividades descritas a continuación: 7.1.1 El Coordinador de la Mesa de ayuda debe contestar el teléfono, siempre debe tener abierta la herramienta de registro de casos, para ir registrando la solicitud mientras atiende al usuario. 7.1.2 Se registra y clasifica la información, de acuerdo con los datos entregados por el usuario, el Coordinador de Mesa de ayuda se debe asegurar de haber entendido perfectamente el problema, haciendo preguntas puntuales, que permitan esclarecer la incidencia reportada. La descripción debe ser clara y puntual. Las prioridades del caso, son definidas por el coordinador de la mesa de ayuda con base en las políticas de atención a los usuarios, una vez lleguen a un acuerdo con el usuario, pues de ello depende el tiempo de la solución al tipo de problema reportado. 7.1.3 El caso quedará en estado registrado y se enviará una notificación automática via mail al Coordinador IT/Especialista encargado del caso. 7.1.4 El coordinador intentará, en los casos que sea viable, dar solución inmediata al cliente. El tiempo de permanencia en la línea con el usuario no debe superar los 15 minutos, si en este tiempo no es posible dar una solución el encargado del soporte, se debe desplazar al sitio del usuario (en caso de ser posible). Toda la operación debe quedar debidamente registrada en la solución del caso en salesforce.	Area IT

Anexo E. (Continuación)

	IT **ATENCION AL USUARIO IT**	

7.1.5 En caso de ser necesario se dará una explicación al usuario de la falla y cómo puede resolver él mismo el problema si se vuelve a presentar. 7.1.6 La persona que tome el caso, es inmediatamente el responsable de la solicitud hasta que ésta termine. Si la solución al caso toma más tiempo del estimado, deberá notificar al usuario el nivel del avance y el motivo por el cual este tomara más tiempo del estimado. 7.1.7 En caso de que el usuario no se encuentre disponible en el momento de la visita, se notificará mediante mail en avances del caso informando la fecha y hora que se realizó la visita y actualizando el estado del caso a "Espera Usuario".	
7.2 Notificación de cierre de caso. Una vez atendida la solicitud y el problema haya sido resuelto, se debe colocar el caso en estado "Solucionado" y el usuario tiene 48 horas para reabrirlo en caso que no esté satisfecho con la solución dada, después de este tiempo el caso quedará cerrado automáticamente.	Área IT

7. Relación de novedades y cambios

Fecha	Versión	Elaborado por:	Revisado por:	Aprobado por:	Modificación del documento
04-10-12	1	Pedro Siatova/Coord. Tecnología	Sarely López/Calidad	María Cortes/Gerente E	Elaboración inicial
15-07-13	2	O.Hernández /Dir. Calidad	F. Otalora/Dir. Tecnología	W. Ayala/Gerente	Actualización
27-7-16	3	O.Hernández /Dir. Calidad	C. Alcalá/Dir. Tecnología	C. Alcalá/Dir. Tecnología	Actualización

Anexo F. Procedimiento de gestión de recursos tecnológicos

CLC	**IT GESTION RECURSOS TECNOLOGICOS**	gaz

1. **Objetivos:** Explicar los pasos utilizados en la asignación, cambio o devolución de equipos tecnológicos a los empleados de CLC, por parte del área de IT y Administradores de plantas y depósitos.

2. **Alcance:** Este procedimiento es aplicable desde la solicitud hasta la entrega del equipo de cómputo a los empleados de la compañía que requieran equipos tecnológicos y que hayan realizado la solicitud al área de IT.

3. **Responsable:** Director IT, Analistas IT, Administradores de plantas y depósitos, Directores de área, Usuario de equipo.

4. **Definiciones:** Backup: Copia de respaldo.

5. **Documentos Soporte:**
   R5-F003 Acta de Entrega de Recursos Tecnológicos
   R5-F001 Formato Solicitud Recursos Tecnológicos
   R5-I001 Instructivo Respaldo de Información De Estaciones De Trabajo Utilizando Synctoy
   R6-F010 Certificado paz y salvo
   R5-F004 Acta De Devolución Recursos Tecnológicos
   R5-O001 Política De Uso De Recursos Informáticos.

6. **Política:** Los equipos tecnológicos para asignar a usuarios nuevos o para cambio a usuarios activos deben ser solicitados por el jefe inmediato mediante el formato **R5-F001 Formato Solicitud de Recursos Tecnológicos** al área de tecnología quien ingresará los datos del usuario al CRM y posteriormente procederá a la configuración del equipo. Para la asignación de recursos tecnológicos a usuarios que se encuentren en ubicaciones externas, el administrador de la planta o depósito como custodio de dichos activos, será quien entregue estos a los funcionarios que el área de IT autorice, adicionalmente el administrador de la planta o depósito será el responsable de hacer llegar la copia del acta firmada al área de IT, en un tiempo no mayor a 5 días. Una asignación de recursos tecnológicos no tardará más de 3 días posteriores a la fecha de recibido el formato de solicitud.

Anexo F. (Continuación)

7. Descripción de Actividades:

ASIGNACION DE EQUIPOS (usuarios activos y usuarios nuevos)		
7.1 PRIMERA ETAPA (BACKUP DE ARCHIVOS)	**Usuario al que aplica.**	**Responsable.**
7.1.1. Se debe realizar back-up en el servidor de respaldos. De acuerdo con el instructivo **R5-I001 Instructivo Respaldo de Información de Estaciones De Trabajo utilizando Synctoy**.	Usuarios activos.	Usuario Jefe inmediato
7.1.2. Verificar la información específica que va a ser respaldada (información que el usuario ha seleccionado)		
7.1.3. Migrar la información al equipo nuevo.		Analista IT.
7.2 SEGUNDA ETAPA (CONFIGURACION DEL EQUIPO DE COMPUTO)	**Usuario al que aplica**	**Responsable**
7.2.1 Se toma como base para la instalación de aplicativos, la información relacionada en el formato **R5-F001 Formato Solicitud de recursos tecnológicos.**	Usuarios activos y Usuarios Nuevos.	
7.2.2 Se cargará la imagen correspondiente al modelo o referencia del equipo a entregar al usuario. Una vez restaurada la imagen, se comprobarán las aplicaciones configuradas y posteriormente se actualizarán.		Analista IT.
7.2.3 Se realiza una administración del disco local del equipo con el objetivo de generar una partición de datos donde el usuario cuenta con un respaldo de la información en caso de que una de las particiones del disco falle.	Usuarios activos y Usuarios Nuevos.	
7.2.4 Se debe cambiar el nombre de máquina.		
7.2.5 Se crea la cuenta de usuario en el servidor de		

Anexo F. (Continuación)

	directorio activo sin privilegios de administración de acuerdo al perfil del usuario. (Directores o Gerentes).		
7.2.6	Se instalan las herramientas de Ofimática		Analista IT
7.2.7	Se configuran las conexiones de red del equipo (Permitir que el equipo tenga salida a internet y acceso a recursos locales).	Usuarios activos Y Usuarios Nuevos.	
7.2.8	Se instalan aplicaciones secundarias (X-lite), estas aplicaciones son para determinados usuarios.		
7.2.9	Se configura la cuenta de correo electrónico.		
7.3 TERCERA ETAPA (MIGRACION DE ARCHIVOS)		**Usuario al que aplica.**	**Responsable**
7.3.1	Se mueve la carpeta de back-up de archivos creada por el usuario al disco local del equipo.	Usuarios activos.	Analista IT
7.4 CUARTA ETAPA (COMPROBACION DEL SISTEMA)		**Usuario al que aplica.**	**Responsable**
7.4.1.	Comprobación de los archivos migrados, que no presenten errores en el momento de abrirlos con la aplicación requerida.		Analista IT
7.4.2.	Generación de accesos directos a aplicaciones.		Analista IT
7.4.3.	Verificación de las aplicaciones y estado del equipo. El usuario deberá revisar el funcionamiento de las aplicaciones configuradas y el estado del equipo y dar su aceptación.	Usuarios nuevos y Activos.	Analista IT / Usuario

Anexo F. (Continuación)

	IT GESTION RECURSOS TECNOLOGICOS	

7.5 ETAPA FINAL (ENTREGA DEL EQUIPO)		Usuario al que aplica.	Responsable
7.5.1	Registra el número de serie y referencia del recurso tecnológico en el formato **R5-F003 Acta de Asignación de Recursos Tecnológicos**.		Director IT/Analista IT /Administrador de planta o depósito
7.5.2	Verificación de los seriales de los elementos entregados al usuario.		
7.5.3	Firma del usuario como aceptación de la entrega del equipo nuevo y firma la política de recursos informáticos, **R5-O001 Política De Uso De Recursos Informáticos**	Usuarios activos Y Usuarios Nuevos.	Director IT/Analista IT /Administrador de planta o depósito
7.5.4	Se realiza entrega de acta relacionada en numeral 7.5.1 a usuario y se guarda copia en archivo de IT.		Usuario
7.5.5	Una vez entregado el equipo, debe registrarse en la base de datos del CRM para garantizar que la información permanezca actualizada.		Director IT/Analista IT /Administrador de planta o depósito

7.6 DEVOLUCION DEL EQUIPO(RETIRO DE PERSONA O CAMBIO DE EQUIPO)			
	Actividades	Usuario al que aplica.	Responsable
7.6.1	Gestión humana y/o Jefe Inmediato informará con anticipación a la Dirección de IT el retiro de una persona de CLC, en caso contrario el área de IT no se hará responsable del recurso asignado ni de la información que este contenga o a la que tenga acceso.	Usuarios activos	Gestión Humana

Anexo F. (Continuación)

	IT GESTION RECURSOS TECNOLOGICOS	

7.6.2	El área de IT ó los administradores de planta o depósito, se encargarán de recoger el equipo de la persona que se retira, posteriormente tecnología debe ingresar como administrador para iniciar sesión en el equipo, para poder realizar back-up de los archivos. Este backup se copia a un medio de almacenamiento externos (Ej. CD, DVD) entregando una copia al Director de Área (si lo solicita) quien acepta su recepción mediante la notificación por correo electrónico al área de tecnología, adicional el Analista IT guarda una copia de la información en el servidor de Respaldos.		Analista IT/administradores de planta o depósito Área IT
7.6.3	Adicionalmente se deben cancelar los servicios de los cuales las persona que se retira hacia uso, tales como:	Usuarios activos	
	• Suspender la cuenta de correo electrónico que fue asignada a la persona que se retira de la empresa, posteriormente se eliminará 5 días después, tiempo en el cual el jefe inmediato podrá solicitar un backup de los correos de ser necesario.		Analista IT
	• Deshabilitar las cuenta de acceso al servidor de Dominio.		
	• Bloquear el acceso a la red, se elimina el usuario de las aplicaciones, se cambia la clave del CRM si el empleado compartía usuario con otros funcionarios.		Analista IT
	• Liberar la extensión telefónica que tenía el usuario asignada.		
7.6.4	La persona que se retira debe entregar el equipo utilizando el formato **R5-F004 Acta De Devolución Recursos Tecnológicos.**		Usuario

Anexo F. (Continuación)

7.6.5 Verificar que el equipo asignado sea el que fue entregado en el momento de ingresar a la empresa y que se encuentre en buenas condiciones para otorgar un paz y salvo **R6-F010 Certificado paz y salvo por recursos tecnológicos asignados.** 7.6.6 Se validará la reinstalación del sistema operativo del equipo para ser reasignado.		Analista IT/administradores de planta o depósito

7.7 MANEJO DE EQUIPOS POR DAÑOS O PÉRDIDAS.		
Actividades	**Usuario al que aplica.**	**Responsable**
7.7.1 El funcionario o su jefe inmediato informará al área de tecnología mediante una solicitud de servicio en la página de helpdesk o vía correo electrónico sobre alguna falla persistente del equipo asignado.	Usuarios activos	Usuario/Jefe de área
7.7.2 **El área de IT ó los administradores de planta o depósito**, se encargarán de recoger el equipo de la persona que reporta el daño, si el equipo se encuentra fuera de las oficinas de CLC Bogotá este deberá ser enviado al área de tecnología para evaluar su daño y enviar un equipo de repuesto en caso de ser necesario.	Usuarios activos	Analista IT/administradores de planta o depósito
7.7.3 Si los equipos presentan daños que no son corregidos por el área de IT se deberá verificar cual es el daño presentado, si fue por mala manipulación, por accidente o similar para proceder a informar a gestión humana y que este proceda con el descuento del valor del activo, en caso de ser necesario.		Analista IT/administradores de planta o depósito/Gestión Humana

Anexo F. (Continuación)

	IT GESTION RECURSOS TECNOLOGICOS	

7.7.4	Si el costo del equipo es inferior a $1.500.000 se procederá a ser guardado y marcado en las bodegas de IT para una verificación posterior con algún proveedor, y evaluar su arreglo, si el valor del activo o su necesidad es de suma importancia para la operación, como plantas eléctricas, red contra incendios, circuitos cerrados de tv, entre otros, se procederá a cotizar inmediatamente su arreglo y presentar esta solución a la gerencia para su corrección.	Usuarios activos	Analista IT
7.7.5	En caso de pérdida o no devolución de activo, el usuario o jefe de área debe informar al área de IT, el cual procederá a evaluar el costo del activo e informar a Gestión Humana para que proceda con el respectivo cobro.		
7.7.6	Si el usuario se retira de la compañía y no realiza la devolución del equipo asignado este deberá ser cobrado de su liquidación y quedara registrado en el Paz y Salvo. Si el usuario se retira de la compañía y el jefe inmediato no realiza el procedimiento de recepción de activos, estos le serán cobrados a él en caso de pérdida o daño.	Usuarios	Analista IT

8. Relación de novedades y cambios

Fecha	Versión	Creado por:	Revisado por:	Aprobado por:	Modificación del documento
04-10-12	1	Pedro Siatova/Coord. Tecnología	Sarely López/Calidad	María Cortes	Elaboración inicial
22-03-13	1	Olga Hernández/Dir. Calidad F. Otalora / Dir. Tecnología	F. Otalora / Dir. Tecnología	W.Ayala/Gerente	Modificación procedimiento Agregado punto 7.7

Anexo G. Procedimiento de seguimiento de software instalado

CLC	**SEGUIMIENTO DE SOFTWARE INSTALADO**	gaz

1. **Objetivos**: Describir los pasos para revisar y mantener un control de los productos de software instalados en los equipos de la compañía mediante el uso de la herramienta de gestión OCS Inventory.

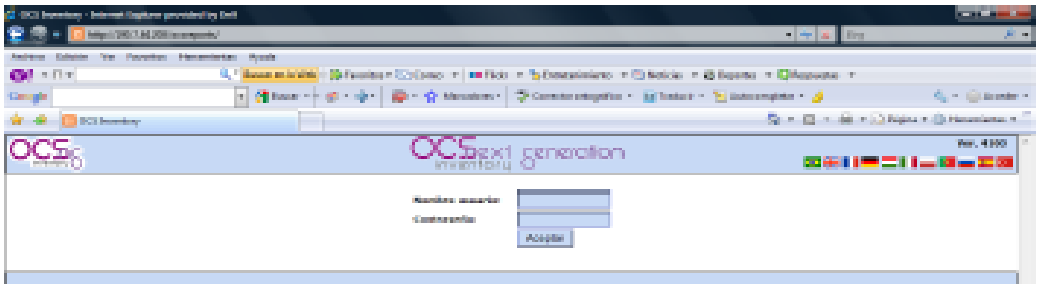
2. **Alcance**: Todos los equipos de cómputo usuario interno de la compañía.

3. **Responsables**: Líder: Director IT
   Coordinador IT

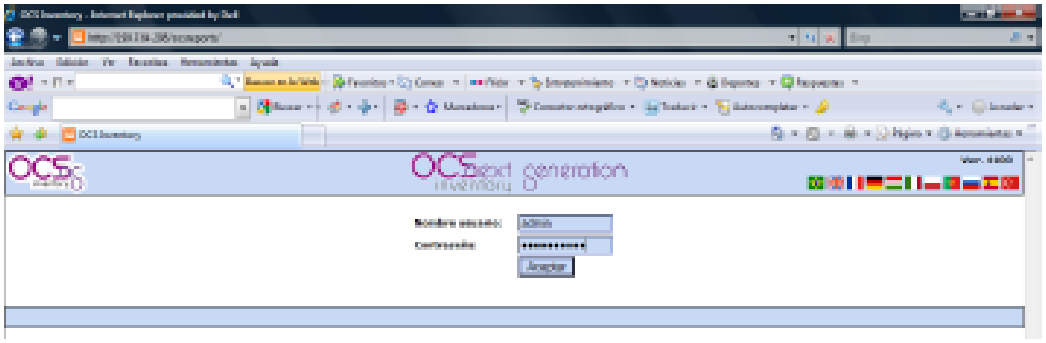
4. **Documentos soportes**: R5-F007 Revisión de Software

5. **Descripción de actividad**: Disposiciones generales: Para el desarrollo de este instructivo se debe contar con el software de gestión OCS Inventory, el cual centraliza de forma automática la información correspondiente al software instalado en cada uno de los equipos de cómputo de la compañía.

6. **Desarrollo**:
   6.1. Acceder a la consola OCS-NG ingresando a la dirección
   http://192.168.38.12/ocsreports/



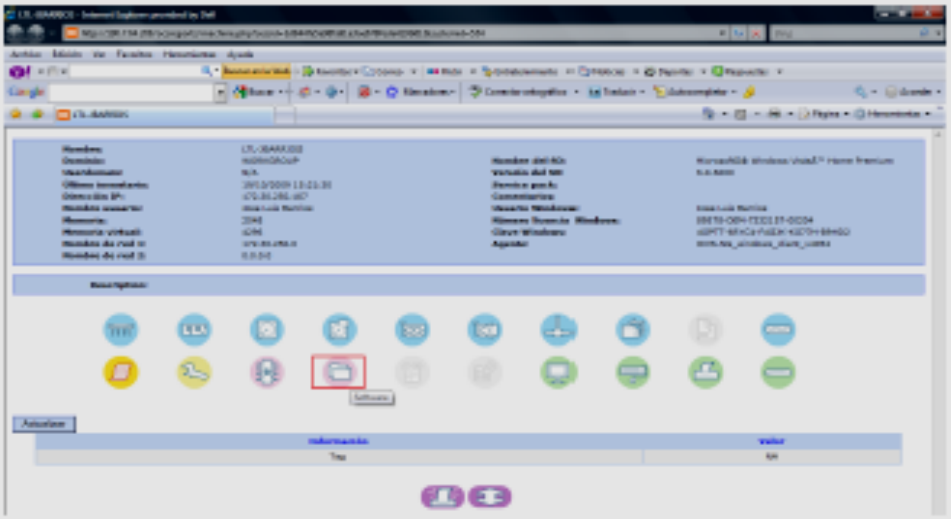
6.2 Utilizar las credenciales de administrador para ingresar a la consola.



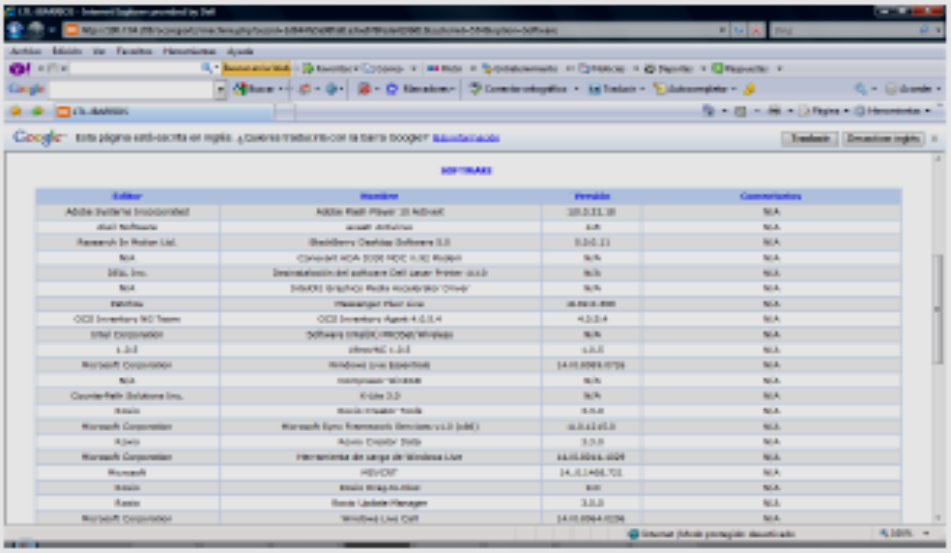
Anexo G. (Continuación)

CLC	SEGUIMIENTO DE SOFTWARE INSTALADO	gaz

6.5. Seleccionar el Icono de software.



6.6. Una vez se ingresa a este Icono se desplegará una lista con todo el software instalado en el equipo.



Anexo H. Procedimiento para registro de casos de mesa de ayuda

CLC	**INSTRUCTIVO PARA CASO MESA DE AYUDA**	gaz

1. **Objetivo:** Explicar los pasos utilizados para la creación de casos de la mesa de ayuda.
2. **Alcance:** Este instructivo es aplicable a todo el personal de la compañía.
3. **Responsables:** Líder: Director IT, Coordinador IT, Directores de área, Usuario de equipo.
4. **Descripción de Actividades:**

4.1. Ingrese a la URL http://clcgas.force.com/helpdesk

Como se visualiza en la siguiente imagen

Nombre: Ingresa nombre y apellido del usuario

Correo electrónico: Ingrese su cuenta de correo corporativa

Celular: Ingresa numero celular corporativo (si lo tiene)

Asunto: Describa el tipo de soporte

Describa su solicitud: Detalle el inconveniente o solicitud de manera detallada

Anexo H. (Continuación)

Finalice con la opción "Enviar" a vuelta de correo recibirá un mail de confirmación del registro del caso.

5. Relación de novedades y cambios

Fecha	Versión	Creado por:	Revisado por:	Aprobado por:	Modificación del documento
04-10-12	1	Pedro Siatova/Cood. Tecnología	Sarely López/Calidad	Maria Cortes/Gerente E	Elaboración inicial

Anexo I. Instructivo de respaldo de información de estaciones de trabajo

CLC	***INSTRUCTIVO BACKUP DE INFORMACION UTILIZANDO SYNCTOY***	gaz

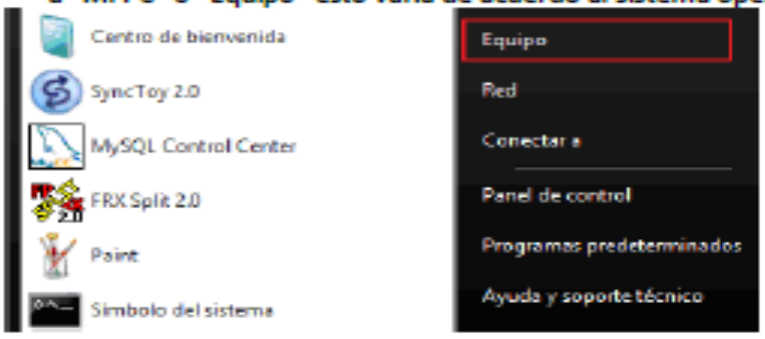
1. **Objetivo**:
   Establecer los pasos que deben seguir los funcionarios de CLC para la realización periódica de Backup en sus equipos de cómputo.

2. **Alcance: Este instructivo aplica para la Oficina principal de CLC en Bogotá.**

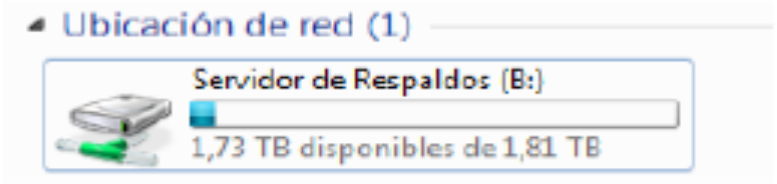
3. **Responsables: Líder: Director IT, Coordinador IT, Directores de área, Usuario de equipo.**

4. **Descripción de Actividades:**

   a. **Ingrese a su equipo y verifique que tenga acceso a la unidad de respaldos, diríjase a "Mi PC" ó "Equipo" esto varía de acuerdo al sistema operativo utilizado.**



   b. **Busque dentro de "Equipo" ó "Mi PC" la unidad llamada Servidor de Respaldos según las credenciales entregadas por el área de Tecnología, si no la encuentra comuníquese con el departamento IT quienes le ayudaran a realizar las conexiones. Recuerde que para ingresar a este recurso de red usted debe ser un usuario autenticado en el servidor de Dominio.**



   c. **Si ya tiene la unidad configurada diríjase a "Programas" y busque el programa que ya tiene instalado en su equipo llamado "SyncToy" y dé clic sobre su icono.**

Anexo I. (Continuación)

CLC	***INSTRUCTIVO BACKUP DE INFORMACION UTILIZANDO SYNCTOY***	gaz

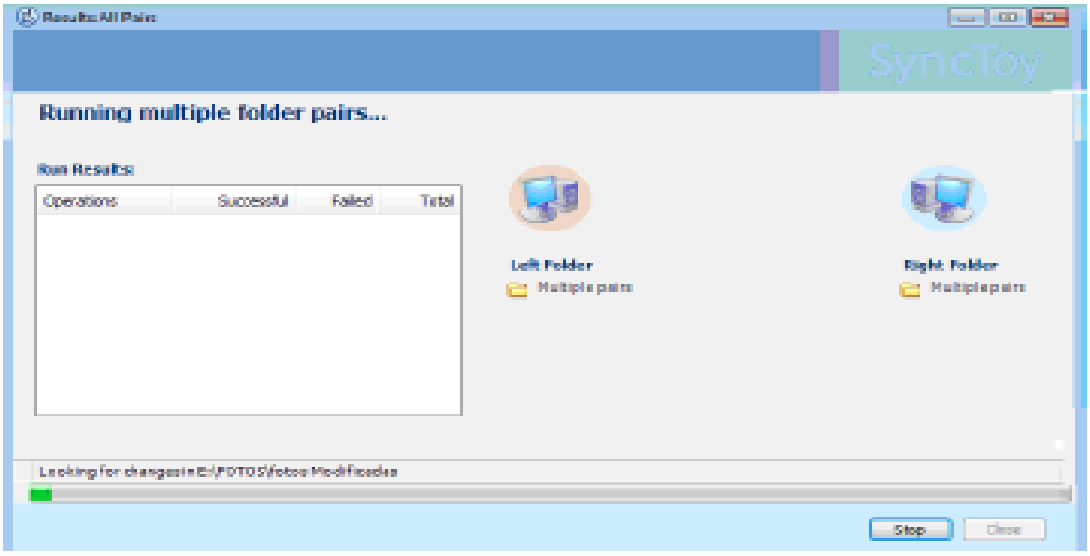
SyncToy

d. Seguido a la acción anterior se le presentará una imagen en la cual le pedirá que especifique a que le realizará backup, esta configuración ya deberá estar establecida en su equipo, si no está disponible comuníquese con el área de Tecnología quien le colaborará para realizar esta labor.

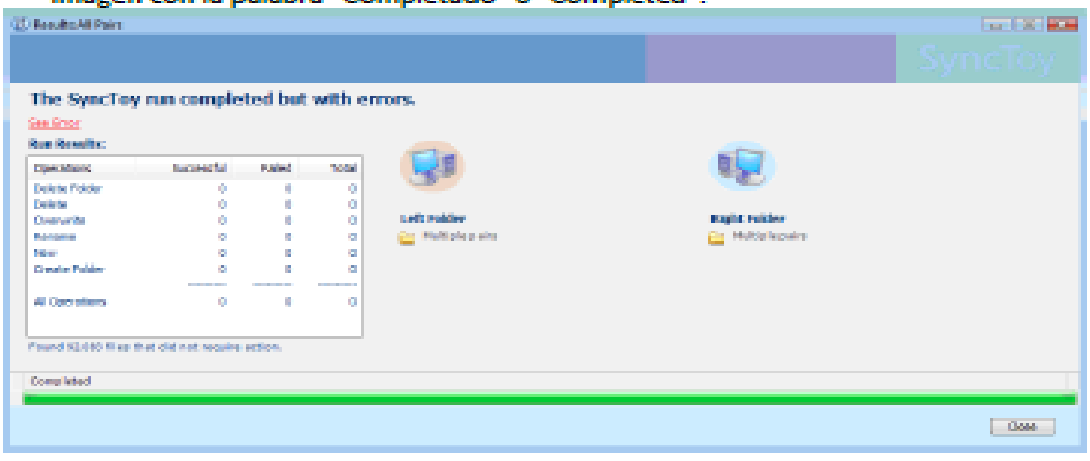
e. Seguido a esto dé clic en "Run" el cual ejecutará los respaldos de las carpetas seleccionadas en la parte superior.

Anexo I. (Continuación)

CLC	***INSTRUCTIVO BACKUP DE INFORMACION UTILIZANDO SYNCTOY***	gaz



f. La imagen anterior es como se mostrará el avance del proceso de respaldos sobre la herramienta de SyncToy, debemos esperar hasta que nos salga la siguiente imagen con la palabra "Completado" ó "Completed".



g. Con la imagen completa, daremos clic en "Cerrar" ó "Close" y de esta manera estará finalizado nuestro respaldo de información.

Anexo I. (Continuación)

	INSTRUCTIVO BACKUP DE INFORMACION UTILIZANDO SYNCTOY	

Como recomendación final el área de tecnología indica que es importante efectuar este backup con una periodicidad semanal con el fin de mantener actualizada la información que permanecerá en el servidor de respaldos.

5. Relación de novedades y cambios

Fecha	Versión	Creado por:	Revisado por:	Aprobado por:	Modificación del documento
27-09-12	1	Pedro Siatova	Sarely López	Maria Cortes	Elaboración inicial
15-07-13	2	O. Hernández/ Dir. Calidad	F. Otalora / Dir. Tecnología	W. Ayala / Gerente	Modificación del alcance.

Anexo J. Formato para seguimiento de software

REVISION DE SOFTWARE

NOMBRE DEL PC	RESPONSABLE	SOFTWARE NO VALIDO	FECHA INSTALACION	FECHA REVISION	ACCION CORRECTIVA

Anexo K. Formato para planilla de inventario

REPORTE DE INVENTARIO IT								
CODIGO INVENTARIO	SERIAL EQUIPO	NOMBRE DEL RESPONSABLE	MARCA	REFERENCIA	ESTADO	UBICACIÓN	FECHA REVISIÓN	OBSERVACIONES

Anexo L. Formato para control de cambios

CONTROL DE CAMBIOS

DEPARTAMENTO DE IT

Fecha:	Responsable:
Objetivo:	Cargo:
	Area:
Nivel de Impacto:	

LISTADO DE ACTIVIDADES		
TAREA	**RESPONSABLE**	**FECHA**
1.		
2.		
3.		
4.		
5.		
6.		
7.		

ACTIVIDADES REALIZADAS

Responsable: **Aprobado:**

Coordinador Director de Tecnología

Anexo M. Formato acta de devolución de equipos tecnológicos

CLC	ACTA DE DEVOLUCION EQUIPOS DE COMPUTO	gaz

LUGAR Y FECHA: _____

Yo, _____ con documento de identidad No._____ de _____ realizo entrega a la Dirección de Tecnología los elementos de cómputo abajo relacionados, los cuales se encontraban bajo mi responsabilidad.

RELACIÓN DE DEVOLUCIÓN

Marca	Referencia	Tipo	Cod. Inventario	Serial

Todos los elementos deben ser devueltos a la Dirección de Tecnología con sus empaques originales y accesorios.

Observaciones *(espacio exclusivo tecnología)*:

ENTREGADO POR:

_____
Nombres y apellidos

RECIBIDO POR:

_____
Nombres y apellidos

Anexo N. Formato de acta de entrega de equipos tecnológicos

CLC	**ACTA DE ENTREGA DE EQUIPOS TECNOLOGICOS**	gaz

Lugar Y Fecha:

Los equipos y elementos relacionados a continuación son propiedad de COMBUSTIBLES LÍQUIDOS DE COLOMBIA S.A. E.S.P., se recomienda hacer buen uso de los mismos, En caso de pérdida o daño los equipos se deben reportar en un plazo mínimo de 5 días hábiles, de no ser así se realizara el cobro por el valor total de la reposición o reparación que cubra los bienes afectados,
El valor de la pérdida o daño será asumido por el funcionario y será descontado de su nómina.

Por políticas de seguridad de la información de la compañía se señala que: El uso de Software no autorizado o adquirido ilegalmente, es considerado como PIRATA y por tanto una violación a los derechos de autor. Todas las áreas de COMBUSTIBLES LÍQUIDOS DE COLOMBIA S.A. E.S.P. podrán utilizar únicamente el hardware y el software que el departamento de tecnología le haya instalado y oficializado mediante el "Acta de entrega de Recursos Tecnológicos". Toda necesidad de hardware y/o software adicional debe ser solicitada por requerimiento al departamento de tecnología, quien justificará o no dicha solicitud, mediante un estudio evaluativo. Tanto el hardware y software, como los datos, son propiedad de la empresa, su copia, eliminación, daño intencional o utilización para fines distintos a las labores propias de la compañía, será sancionada de acuerdo con las normas y reglamento interno de la empresa.

RELACIÓN DE ENTREGA

Marca	Referencia	Tipo	Cod. Inventario	Serial

Observaciones:
Todos los elementos deben ser devueltos a la Dirección de Tecnología con sus empaques originales y accesorios.

ENTREGADO POR:

_____
Nombres y apellidos

AUTORIZACION DE DESCUENTO: Autorizo a COMBUSTIBLES LIQUIDOS DE COLOMBIA S.A. E.S.P., descontar de la nómina mensual y/o liquidación definitiva del contrato de trabajo y prestaciones sociales, el valor correspondiente por perdida del activo relacionado en este documento, y por los consumos adicionales del servicio de celular asignado para el desarrollo de mis funciones.

_____ _____
(NOMBRES Y APELLIDOS) (Firma)

_____
CENTRO DE OPERACIÓN

Anexo O. Formato de hoja de vida de equipos de cómputo

FICHA TECNICA DE EQUIPO DE COMPUTO

Usuario:				
Identificacion:			**Telefono:**	
Tipo de Computador:	**PC**	**Portatil**	**Marca:**	**Serial:**

HARDWARE

Main Board:	Marca:	Modelo:	
	Puertos Pci:	Puertos USB:	VGA:
	Red RJ45:	Otro:	Otro:

DESCRIPCION	MARCA	CAPACIDAD O MODELO
Disco Duro 1 Tipo		
Disco Duro 2 Tipo		
Procesador:		
RAM TOTAL:		
Unidad DVD		
Unidad CD		
Monitor:		

SOFTWARE

DESCIPCION:	NOMBRE	VERSION	LICENCIA
Sistema Operacional:			
Sistema Ofimatico:			
Compresor:			
Quemador:			
Programa 1 de Diseño:			
Programa 2 de Diseño:			
Programas P2P:			
Antivirus:			
Programa de aplicación:			
Programa de aplicación:			
Programa de aplicación:			
Programa de aplicación:			
Programa de aplicación:			
Programa de aplicación:			

Usuario que tiene asignado el equipo: *Quien Realiza el mantenimiento:*

R5-F002
V2/29-12-14/

Anexo O. (Continuación)

HOJA DE VIDA DEL COMPUTADOR

Mantenimiento Fisico	Mantenimiento Software
Fecha:	Fecha:
Labores realizadas:	Labores realizadas:
Cambio de Partes:	**Cambios a los programas:**

Mantenimiento Fisico	Mantenimiento Software
Fecha	Fecha
Labores realizadas	Labores realizadas
Cambio de Partes	**Cambios a los programas**

Mantenimiento Fisico	Mantenimiento Software
Fecha	Fecha
Labores realizadas	Labores realizadas
Cambio de Partes	**Cambios a los programas**

R5-F002
V2/29-12-14/

Anexo P. Formato de solicitud de recursos tecnológicos

	FORMATO SOLICITUD DE RECURSOS	

Persona que solicita:	
Fecha Solicitud:	
Nombre Completo usuario:	
Número de cédula Usuario:	
Área a la que ingresa:	
Cargo al que ingresa:	
Sede principal:	
Fecha de Ingreso:	

Seleccione todas las herramientas y/o servicios tecnológicos a los cuales el usuario debe tener acceso:

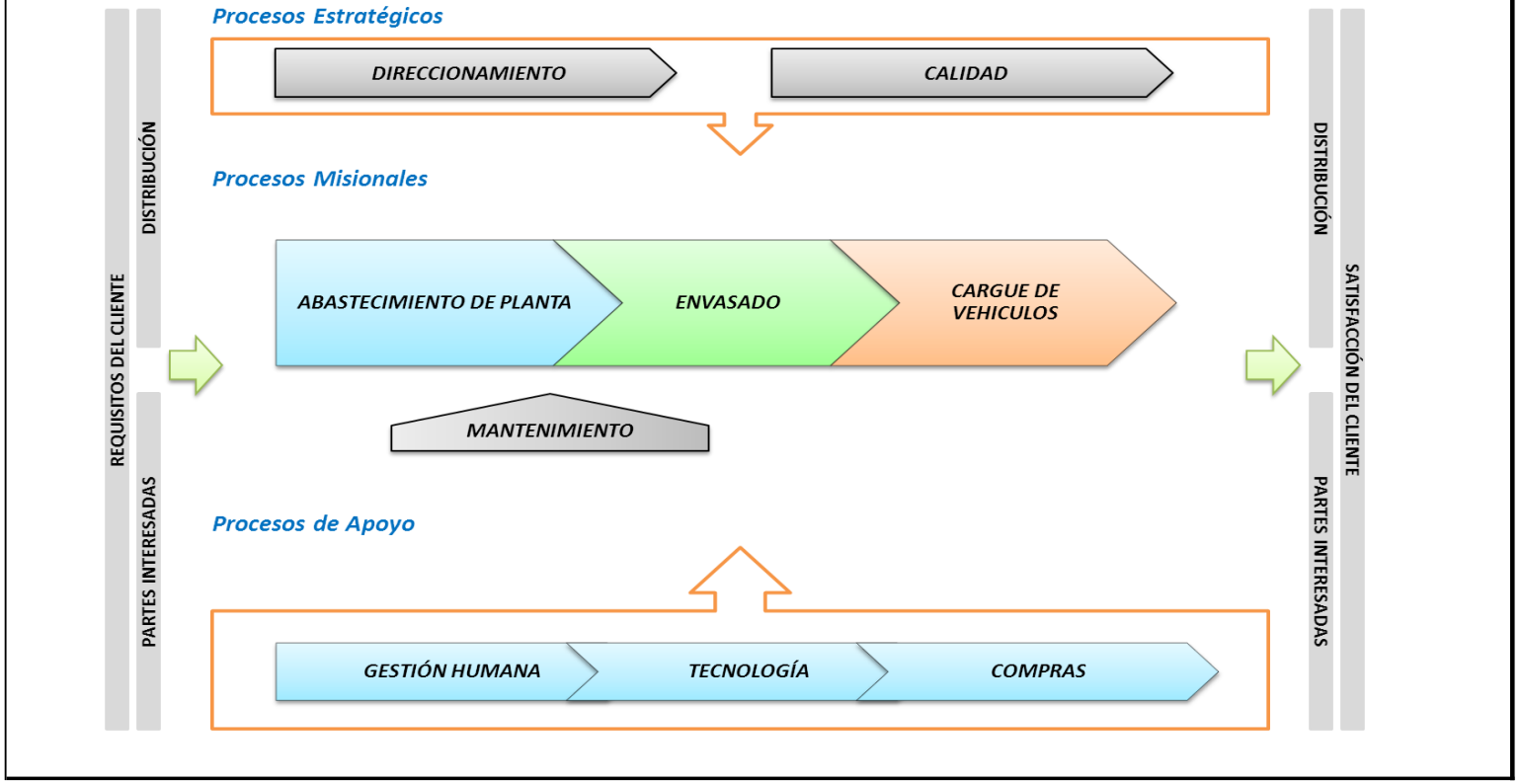
CONCEPTO	SI	NO	OBSERVACIONES
Equipo de Cómputo			
Computador de Escritorio	☐	☐	
Computador Portátil	☐	☐	
Herramientas Ofimáticas			
Microsoft Office (Excel, Word, PowerPoint)	☐	☐	
Otras	☐	☐	
Telefonía			
Extensión IP	☐	☐	
Celular corporativo	☐	☐	
Herramientas Corporativas			
Sistema CGUno	☐	☐	
SalesForce	☐	☐	
Dyalogo	☐	☐	
ArcGis	☐	☐	
Autocad	☐	☐	
QlickView	☐	☐	
Saasmaint	☐	☐	
Aplicación Seguimiento satelital	☐	☐	
Herramientas Mensajería			
Google Talk	☐	☐	
Skype	☐	☐	
Correo Electrónico			
Cuenta de correo	☐	☐	
Grupo de Correo	☐	☐	
Carpetas Compartidas	☐	☐	
¿Cuáles?			
Tarjeta de Acceso	☐	☐	

Firma persona que solicita:	
Firma Analista IT que recibe:	**Fecha de recepción:**

Anexo Q. Caracterización del proceso de tecnología

MAPA DE PROCESOS SGC

Combustibles Líquidos de Colombia ha identificado los siguientes procesos:



Anexo Q. (Continuación)

	CARACTERIZACIÓN DE PROCESOS - TECNOLOGÍA	

OBJETIVO DEL PROCESO	Prestar el servicio de administración y soporte de la infraestructura tecnológica y sus plataformas, para asegurar el funcionamiento operativo de la compañía.
ALCANCE DEL PROCESO	Todos los Procesos
TIPO DE PROCESO	**Estrategico** ☐ **Misional** ☐ **Apoyo** ☒
RESPONSABLE DEL PROCESO	Coordinador de Tecnología

PROVEEDORES	ENTRADAS	ACTIVIDADES		SALIDAS	CLIENTES
		ACTUAR	**PLANEAR**		
* Todos los Procesos. * Proveedores Tecnológicos	* Requerimientos de la Mesa de Ayuda. * Lineamientos Gerenciales * Requerimientos de Proveedores	* Definir y solicitar los recursos necesarios para dar solución a las fallas evidenciadas en el mantenimiento de los equipos. * En caso de presentarse cambios en los procesos actualizar y redefinir las políticas de Recursos Informaticos. * Corregir las fallas en la configuración de las plataformas hasta cumplir los requerimientos.	* Asegurar la Administración de los equipos tecnológicos y de las Aplicaciones * Planear el Mantenimiento de los equipos en Plantas (Infraestructura). * Gestionar la Inspeccción de Inventario de equipos tecnológicos	* Cierre de las solicitudes de Servicios (Helpdesk). * Aplicación de las Configuraciones. * Entrega de Activos Fijos. * Ejecución del programa de mantenimiento. Registros	* Todos los Procesos. * Proveedores Tecnológicos
		VERIFICAR	**HACER**		
		* Identifican las fallas que existan en la infraestructura. * Evaluar las políticas de Recursos Informaticos. * Evaluar la gestión realizada por el proveedor de soporte de infraestructura. * Verificar que las configuraciones cumplan con los requerimientos iniciales. * Evaluar el requerimiento de mesa de ayuda, definir prioridad de solución y responsable para dar solución.	* Ejecución del programa de mantenimiento de equipos * Definir las políticas de Recursos Informaticos. * Programación de contratistas para realizar soporte y mejoras a la infraestructura. * Realizar configuraciones sobre las diferentes plataformas. * Realizar Revisión física de Inventarios. * Gestión de Requerimientos Atención Mesa de Ayuda. * Entrega de Recursos Tecnológicos.		

RECURSOS	DOCUMENTOS DEL SGC	REQUISITOS NORMA ISO 9001:2008
Recursos Tecnológicos: - Equipos: Computadores, Telefonicos. - Software: Salesforce, Qlikview, CGUNO, Saasmaint, Arcgis. Recursos Locativos: Infraestructura Recurso Humano.	Documentos Publicados en Plataforma Sites - TECNOLOGÍA	4.2.3 Control de Documentos 4.2.4 Control de Registros 6.3 Infraestructura. 8.2.3 Seguimiento y Medición de los Procesos. 8.5 Mejora

PARAMETROS DE MEDICIÓN

NOMBRE DEL INDICADOR	FORMULA	META	FRECUENCIA
Nivel de Atención Casos Helpdesk	Promedio horas solución	**≤ 36 horas**	Mensual

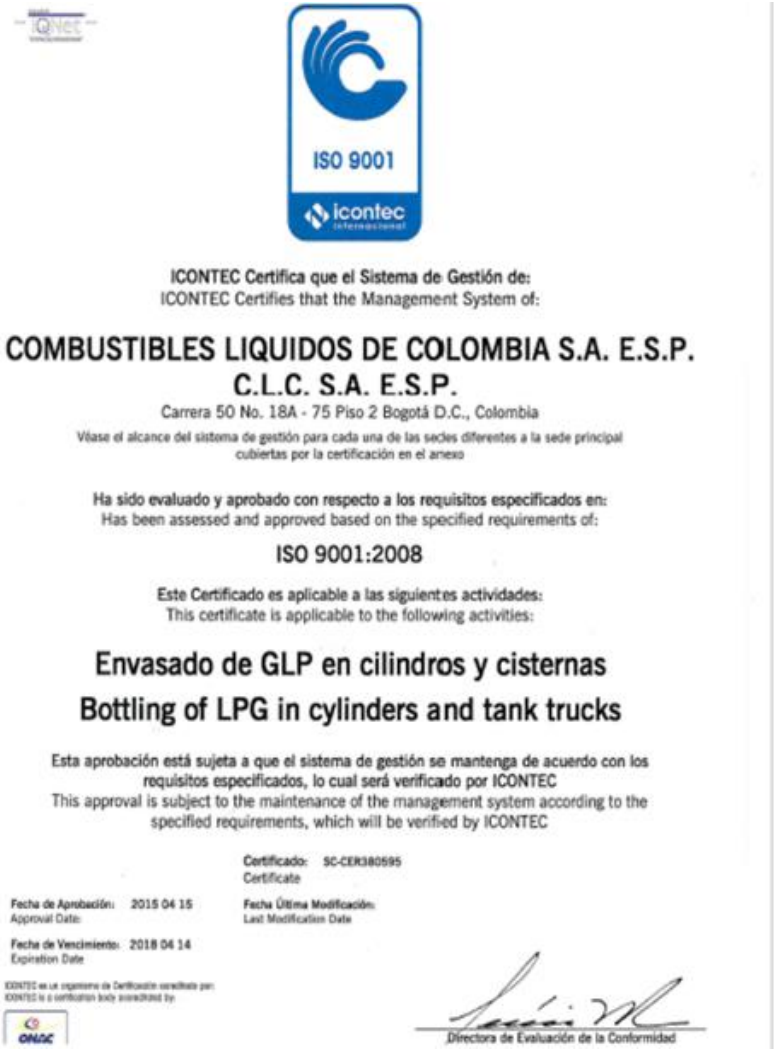
CONTROL DE CAMBIOS

Fecha	Versión	Elaborado por:	Revisado por:	Aprobado por:	Página/Capitulo	Modificación
05/06/2013	1	Olga Hernández / Dir. de Calidad	Francisco Otalora / Dir. De Tecnología	W. Ayala / Gerente	Todas	Creación
09/10/2013	2	Olga Hernández / Dir. Calidad	Francisco Otalora / Dir. De Tecnología	W. Ayala / Gerente	Todo	Evaluación de Indicadores SGC

R12 - F004
V1/29-05-2013/

Anexo R. Sistema de Gestión de calidad de Combustibles Líquidos de Colombia S.A. ESP

Anexo R. (Continuación)



ISO 9001

icontec

ICONTEC Certifica que el Sistema de Gestión de:
ICONTEC Certifies that the Management System of:

COMBUSTIBLES LIQUIDOS DE COLOMBIA S.A. E.S.P.
C.L.C. S.A. E.S.P.

Carrera 50 No. 18A - 75 Piso 2 Bogotá D.C., Colombia

Véase el alcance del sistema de gestión para cada una de las sedes diferentes a la sede principal cubiertas por la certificación en el anexo

Ha sido evaluado y aprobado con respecto a los requisitos especificados en:
Has been assessed and approved based on the specified requirements of:

ISO 9001:2008

Este Certificado es aplicable a las siguientes actividades:
This certificate is applicable to the following activities:

Envasado de GLP en cilindros y cisternas
Bottling of LPG in cylinders and tank trucks

Esta aprobación está sujeta a que el sistema de gestión se mantenga de acuerdo con los requisitos especificados, lo cual será verificado por ICONTEC
This approval is subject to the maintenance of the management system according to the specified requirements, which will be verified by ICONTEC

Certificado: SC-CER380595
Certificate

Fecha de Aprobación: 2015 04 15
Approval Date:

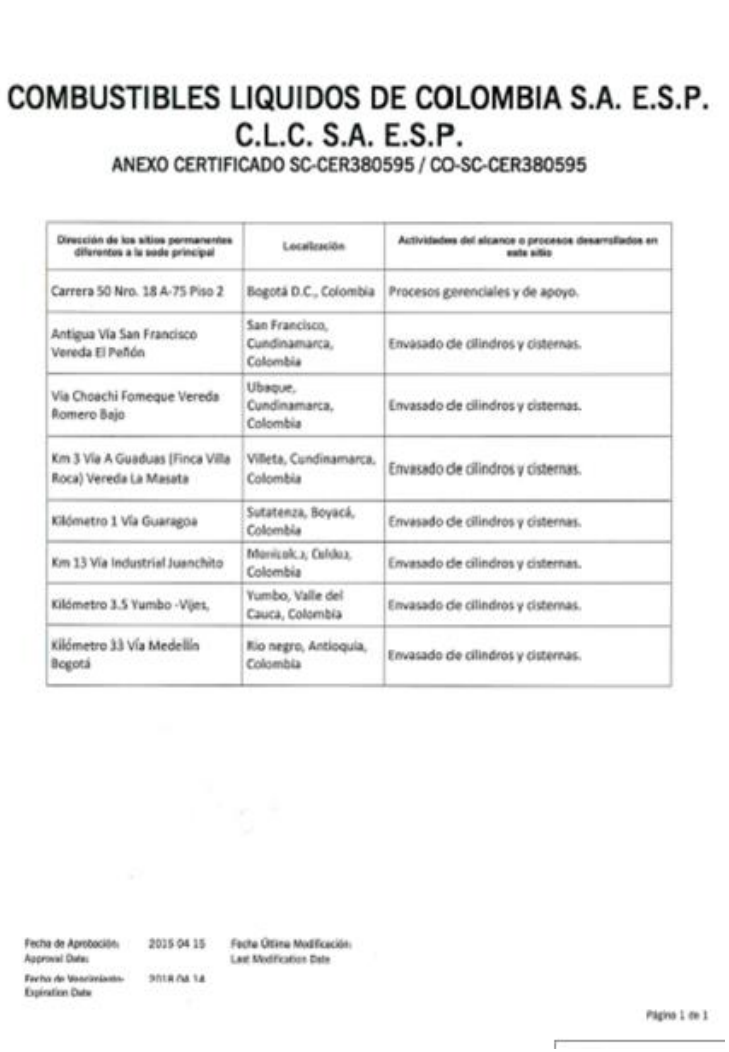
Fecha Última Modificación:
Last Modification Date

Fecha de Vencimiento: 2018 04 14
Expiration Date

ICONTEC es un organismo de Certificación acreditado por:
ICONTEC is a certification body acreditated by:

ONAC

Directora de Evaluación de la Conformidad



COMBUSTIBLES LIQUIDOS DE COLOMBIA S.A. E.S.P.
C.L.C. S.A. E.S.P.
ANEXO CERTIFICADO SC-CER380595 / CO-SC-CER380595

Dirección de los sitios permanentes diferentes a la sede principal	Localización	Actividades del alcance o procesos desarrollados en este sitio
Carrera 50 Nro. 18 A-75 Piso 2	Bogotá D.C., Colombia	Procesos gerenciales y de apoyo.
Antigua Vía San Francisco Vereda El Peñón	San Francisco, Cundinamarca, Colombia	Envasado de cilindros y cisternas.
Vía Choachí Fomeque Vereda Romero Bajo	Ubaque, Cundinamarca, Colombia	Envasado de cilindros y cisternas.
Km 3 Vía A Guaduas (Finca Villa Roca) Vereda La Masata	Villeta, Cundinamarca, Colombia	Envasado de cilindros y cisternas.
Kilómetro 1 Vía Guaragoa	Sutatenza, Boyacá, Colombia	Envasado de cilindros y cisternas.
Km 13 Vía Industrial Juanchito	Monikokia, Caldas, Colombia	Envasado de cilindros y cisternas.
Kilómetro 3.5 Yumbo -Vijes,	Yumbo, Valle del Cauca, Colombia	Envasado de cilindros y cisternas.
Kilómetro 33 Vía Medellín Bogotá	Rio negro, Antioquia, Colombia	Envasado de cilindros y cisternas.

Fecha de Aprobación: 2015 04 15
Approval Date:

Fecha Última Modificación:
Last Modification Date

Fecha de Vencimiento: 2018 04 14
Expiration Date

Página 1 de 1