RESUMEN – TRABAJO DE GRADO

AUTORES	AXEL ALONSO CARREÑO SUAREZ JESSENIA ROMERO SAMPAYO
FACULTAD	DE INGENIERIAS
PLAN DE ESTUDIOS	ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS
DIRECTOR	YESICA MARÍA PEREZ PEREZ
TÍTULO DE LA TESIS	PLAN DE GESTION DE RIESGOS DE LA EMPRESA D.R.G TOTAL SERVICIOS ENERGY S.A.S EN LA CIUDAD DE AGUACHICA CESAR, BASADO EN LA NORMA NTC ISO 270001:2013

RESUMEN
(70 palabras aproximadamente)

EN LA ACTUALIDAD SE HA HECHO IMPRESCINDIBLE QUE, SIN IMPORTAR EL TAMAÑO DE LA EMPRESA SE IMPLEMENTEN ESTRATEGIAS QUE AYUDEN A GESTIONAR DE MEJOR MANERA LOS RECURSOS ORGANIZACIONALES, ENTRE ELLOS LA INFORMACIÓN, DE ACUERDO CON ESTO LA PRESENTE INVESTIGACIÓN ABORDA EL TEMA DE LOS RIESGOS DE LA INFORMACIÓN COMO HERRAMIENTA ESTRATÉGICA PARA UNA EMPRESA DE SERVICIOS DE ASESORÍA Y CONSULTORÍA. EL PROPÓSITO DEL ESTUDIO CONSISTE EN PROPONER UN PLAN DE GESTIÓN DE RIESGOS BASADO EN LA NORMA NTC ISO 27001:2013.

CARACTERÍSTICAS

PÁGINAS: 75	PLANOS: 0	ILUSTRACIONES: 5	CD-ROM:1

PLAN DE GESTION DE RIESGOS DE LA EMPRESA D.R.G TOTAL SERVICIOS ENERGY S.A.S EN LA CIUDAD DE AGUACHICA CESAR, BASADO EN LA NORMA NTC ISO 270001:2013

AUTORES

AXEL ALONSO CARREÑO SUAREZ

JESSENIA ROMERO SAMPAYO

Proyecto de grado como requisito para obtener el grado de Especialista en Auditoria de Sistemas

DIRECTOR

YESICA MARÍA PEREZ PEREZ

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER

FACULTAD DE INGENIERIAS

ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS

Ocaña, Colombia **Noviembre, 2019**

Dedicatorias

A Dios, por permitirme llegar en este momento por los triunfos y los momentos difíciles que me han enseñado a valorarlo cada día más.

A mis hijos, que son la luz de mi vida, los que me animan salir adelante, valiente y cada día ser una mejor persona

A mi esposa por su comprensión y apoyo incondicional en mis estudios.

Mis padres por enseñarme no derrotarme nunca, ser honesto, responsable transparente con mi vida y la profesión

A todos los docentes por su aporte a nuestra formación profesional durante el proceso de la especialización.

Axel Alonso Carreño Suarez

El presente trabajo investigativo lo dedico principalmente a Dios, por ser el inspirador y darme fuerza para continuar en este proceso de obtener uno de mis anhelos más deseados.

A mis padres, por su amor, trabajo y sacrificio en todos estos años, gracias a ustedes he logrado llegar hasta aquí y convertirme en lo que soy. Ha sido el orgullo y el privilegio de ser su hija, son los mejores padres.

A todas las personas que me han apoyado y han hecho que el trabajo se realice con éxito en especial a aquellos que abrieron las puertas y compartieron sus conocimientos.

Jessenia Romero Sampayo.

Agradecimientos

Agradecimientos a todos los docentes por su aporte a nuestra formación profesional durante el proceso de la especialización.

Axel Alonso Carreño Suarez.

Principalmente a Dios por bendecirme siempre en la vida, por guiarme a lo largo de mi existencia, ser el apoyo y fortaleza en aquellos momentos de dificultad y de debilidad.

Gracias a mis padres: José Romero y Justina Sampayo, por ser los principales promotores de mis sueños, por confiar y creer en mis expectativas, por los consejos, valores y principios que me han inculcado.

Agradezco a mis docentes de la Universidad Francisco de Paula Santander - Ocaña, por haber compartido sus conocimientos a lo largo de la preparación para esta especialización, de manera especial, a la Esp. Yesica María Pérez Pérez tutor de nuestro proyecto de investigación quien ha guiado con su paciencia, y su conocimiento como docente.

Sin olvidar a mis amigos, los cuales conocí en este maravilloso proceso.

Jessenia Romero Sampayo.

Índice

Lista de Tablas

Lista de Figuras

Lista de apéndices

Introducción

En la actualidad se ha hecho imprescindible que, sin importar el tamaño de la empresa se implementen estrategias que ayuden a gestionar de mejor manera los recursos organizacionales, entre ellos la información, de acuerdo con esto la presente investigación aborda el tema de los riesgos de la información como herramienta estratégica para una empresa de servicios de asesoría y consultoría.

El propósito del estudio consiste en proponer un plan de gestión de riesgos basado en la norma NTC ISO 27001:2013 con el fin de reducir los riegos asociados a la información y así proporcionar herramientas de gestión.

Actualmente se realizan muchas investigaciones sobre el tema, tanto a nivel nacional como internacional, sin embargo el estado del arte revela que las organizaciones que destinan este tipo de gestiones son grandes empresas y por lo general en empresas estatales.

Se pretende realizar una investigación descriptiva de tipo cualitativo con el fin de diagnosticar el estado actual de la empresa frente a la gestión de riesgos asociados a la información , para así determinar el proceso para la administración y gestión del riesgo y por ultimo diseñar un plan de gestión de riesgos de la empresa D.R.G TOTAL SERVICIOS ENERGY S.A.S

Capítulo 1. Plan de gestión de riesgos de la empresa D.R.G total servicios Energy S.A.S en la ciudad de Aguachica Cesar, basado en la norma NTC ISO 27001:2013

1.1. Planteamiento del problema

De acuerdo a la globalización el éxito de una empresa se basa fundamentalmente en la información que posee, pero esa información debe tener unas características específicas para que realmente genere riqueza, en esencia no es solo tener información, es tener información de calidad. Por lo tanto, el valor de la información se materializa en el contexto de su uso, el cual principalmente sirve para la toma de decisiones. En este sentido la "información se entiende como todo aquello que sirve para poner en manifiesto la situación de un entorno, sus objetivos, resultados y reducir la incertidumbre frente a un proceso de decisión" (de Pablos, 2006, p. 29)

Proteger la información es un problema empresarial en el que la solución es mucho más que implementar tecnología como firewalls y gateways antivirus, y esperar lo mejor. Las empresas deben adoptar un enfoque proactivo para identificar y proteger sus activos más importantes, incluida la información, la tecnología de la información y los procesos críticos del negocio. La gestión del riesgo de seguridad de la información permite a una organización evaluar lo que está tratando de proteger, y por qué, como elemento de apoyo a la decisión en la identificación de medidas de seguridad. Una evaluación integral del riesgo de seguridad de la información debería permitir a una organización evaluar sus necesidades y riesgos de seguridad en el contexto de sus necesidades empresariales y organizativas. Es importante tener en cuenta

que el propósito de los sistemas de información y los datos que contienen es apoyar los procesos de negocios, que a su vez apoyan la misión de la organización. En un sentido muy real, la información es un elemento fundamental que apoya al negocio y su misión, y contribuye a la capacidad de una organización para sostener las operaciones. (Sullivan, 2016)

Actualmente la empresa D.R.G TOTAL SERVICIOS ENERGY S.A.S maneja volúmenes de información considerables pues tiene una amplia oferta de servicios, entre ellos el principal radica en la asesoría del derecho minero, donde se brinda asistencia en la totalidad del trámite de suscripción del contrato de concesión, desde la presentación de la solicitud hasta el registro del contrato de concesión en el registro minero nacional, de igual forma se realiza la representación ante las autoridades mineras competentes, incluyendo asistencia en todos los procedimientos necesarios ante dichas autoridades, así como asesoría legal en el seguimiento y vigilancia de los títulos mineros con el fin de velar por el estricto cumplimiento de las obligaciones derivadas de los mismos.

En este sentido la información de la empresa D.R.G debe garantizar a sus clientes oportunidad, confiabilidad, completitud, pertinencia y utilidad, sin embargo dentro de la empresa no se han determinado, analizado, valorado y clasificado los riesgos a los que dicha información se encuentra expuesta, por lo cual se ve diezmada la capacidad institucional para reducir vulnerabilidades o limitar amenazas. En consecuencia se han presentado casos de pérdida o robo de información, desactualización en la información, falta de conocimiento sobre el manejo de la información por parte de los empleados, entre otros. Esto tiene como efecto que los procesos se

vuelvan más lentos, exista perdida de dinero, de clientes y la más importante, perdida de la imagen empresarial.

1.2. Formulación del problema

¿Cómo un plan de gestión de riesgos basado en la norma NTC ISO 27001:2013 permitirá reducir los riegos asociados a la seguridad de la información de la empresa D.R.G TOTAL SERVICIOS ENERGY S.A.S?

1.3. Objetivos

1.3.1. General. Diseñar un plan de gestión de riesgos basado en la norma NTC ISO 27001:2013 con el fin de reducir los riegos asociados a la información de la empresa D.R.G TOTAL SERVICIOS ENERGY S.A.S

1.3.2. Específicos. Diagnosticar el estado actual de la empresa D.R.G TOTAL SERVICIOS ENERGY S.A.S frente a la gestión de riesgos asociados a la información

Formular el proceso para la administración y gestión del riesgo de la empresa D.R.G TOTAL SERVICIOS ENERGY S.A.S

Planificar la gestión de riesgos de la empresa D.R.G TOTAL SERVICIOS ENERGY S.A.S

1.4. Justificación

D.R.G TOTAL SERVICIOS ENERGY S.A.S como muchas otras empresas colombianas, han iniciado la prestación de sus servicios como microempresas y ha ido evolucionando para consolidarse frente a su mercado, este desarrollo ha permitido que a la fecha cuente con más de 15 clientes y negocie con alrededor de 200 proveedores. Este panorama de crecimiento, implica que la información que se maneje aumente, pero a medida que esta evolución se da, también se deben dar progresiones en los procesos de gestión. De ahí radica la importancia de comprometer a las organizaciones a generar mejores compromisos frente a la calidad de los servicios que prestan, sus tiempos de respuesta y sin duda garantizar que la información que proveen sea veraz y más en el caso de la prestación de servicios

De acuerdo con (Ladino, Villa, & López, 2011), el amplio uso de las tecnologías de información en los negocios hace que cada vez sea más fácil la expansión de éstos. La comunicación con clientes que se encuentran en una ciudad o país diferente al de ubicación de la empresa, la posibilidad de realizar transacciones comerciales vía web y en general, la facilidad del uso de la tecnología y la globalización de la información para todas las personas ha contribuido a que las organizaciones crezcan cada vez más rápido. Sin embargo, toda esta cercanía y facilidad de uso de la tecnología ha generado ciertos problemas a las organizaciones, que día tras día son más vulnerables a las amenazas que se presentan en el medio, las cuales pueden llegar a convertirse en un verdadero riesgo para la organización afectando el correcto funcionamiento de las actividades del negocio. p.54

Por otra parte, es importante recalcar que el estudio de la gestión de riesgos provee conocimientos y toma de buenas prácticas, por lo que esta investigación busca aportar un marco teórico para las futuras aplicaciones del modelo NTC ISO 27000:2013 por medio del caso práctico expuesto en la empresa D.R.G TOTAL SERVICIOS ENERGY S.A.S.

Adicionalmente esta norma adopta el modelo de procesos "Planificar-Hacer-Verificar-Actuar" (PHVA), que se aplica para estructurar todos los procesos del SGSI. Toma como elementos de entrada los requisitos de seguridad de la información y las expectativas de las partes interesadas, y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que cumplen estos requisitos y expectativas. La adopción del modelo PHVA también reflejará los principios establecidos en las Directrices OCDE que controlan la seguridad de sistemas y redes de información. Esta norma brinda un modelo robusto para implementar los principios en aquellas directrices que controlan la evaluación de riesgos, diseño e implementación de la seguridad, gestión y reevaluación de la seguridad. (Iso27000.es, 2013). Finalmente podemos decir que el presente trabajo de investigación se fundamenta en la necesidad de aportes académicos y la ejemplificación de la gestión de riesgos por medio de la generación de conocimientos y el estudio teórico y práctico del tema.

1.5. Hipótesis

La propuesta de un plan de gestión de riesgos en la empresa D.R.G Total Servicios Energy S.A.S basado en la norma NTC ISO 27001:2013 presenta un contexto de la organización,

identifica, analiza y valora el riesgo, así como permite la generación de una política de administración de riesgos.

1.6. Delimitaciones

1.6.1. Geográficas. El proyecto se delimita para la sede de la empresa D.R.G Total Servicios Energy S.A.S ubicada en la ciudad de Aguachica, Cesar. Carrera 11 No. 5ª –76

1.6.2. Temporales. El proyecto se delimita para la información producida por la empresa D.R.G Total Servicios Energy S.A.S en un año. De igual manera para el desarrollo de la investigación se propone un tiempo de tres meses después de la aprobación del anteproyecto.

1.6.3. Conceptuales. El proyecto se delimita en el concepto de gestión del riesgo establecidas por la Guía ISO/IEC 73:2002, y definido como aquellas actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

1.6.4. Operativa. El proyecto se delimita para todos los procesos de asesoría en Derecho, prestados por la empresa D.R.G Total Servicios Energy S.A.S

Capítulo 2. Marco referencial

2.1 Marco histórico

De acuerdo con (Ponjuán, 2011) desde la década de los ´80, la llamada Gestión de Información, Gerencia de Información o Information Management (en inglés) ha ganado un espacio importante en la vida de las instituciones en general y en particular en aquellas que tienen como misión el desarrollo de servicios y productos de información.

En función a diferentes modelos para gestionar la información, es preciso acudir a las normas internacionales que hacen referencia a los sistemas de gestión que permiten asegurar la información como un activo intangible. A nivel internacional se ha desarrollado como principal estándar de seguridad la serie de normas ISO/IEC 27000, que se establece los requisitos por medio de la ISO/IEC 27001 la cual fue publicada en 2005 por la Organización Internacional de Normalización (ISO). Sin embargo de acuerdo al portal (Pmg-ssi.com, 2013)

La historia de la ISO 27001 se remonta a la entidad normalizadora británica BSI (British Standards Institution) con carácter internacional, quien publica la norma que fue su origen, la BS 7799-1, publicada en 1995. Se trataba de una serie de mejores prácticas para ayudar a las empresas británicas a administrar la Seguridad de la Información. Esta norma tuvo una segunda parte, BS 7799-2, en 1998. Es este caso establecía los requisitos a cumplir para tener un Sistema de Gestión de Seguridad de la Información certificable. Ambas partes fueron revisadas en el año 1999 y en el año 2000 la Organización Internacional para la Estandarización (ISO) tomó la

norma británica BS 7799-1 que dio lugar a la llamada ISO 17799. En este momento la norma no experimentó grandes cambios, pero en el año 2001 fue revisada de acuerdo a la línea de las normas ISO. En 2002 se publicó una nueva versión de la BS 7799 que permitió la acreditación de empresas por una entidad certificadora en Reino Unido y en otros países. Fue en el año 2005 cuando aparece ya el estándar ISO 27001 y la ISO 17799 se modifica danto lugar a la ISO 27001:2005 publicación formal de la revisión. En 2007 la ISO 17799 se renombra y pasa a ser la ISO 27002:2005. En 2007 se publica la nueva versión ISO 27001:2007 y dos años más tarde se publica un documento adicional de modificaciones llamado ISO 27001:2007/1M:2009.

A partir de la ISO/IEC 27001:2013 se adopta un enfoque para la gestión del riesgo, básicamente, la seguridad de la información es parte de la gestión global del riesgo en una empresa, hay aspectos que se superponen con la ciberseguridad, con la gestión de la continuidad del negocio y con la tecnología de la información. (Advisiera Expert Solution Ltd, 2013)

Figura 1. Gestión del riesgo. Fuente Advisiera.com

En Colombia el Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, es el organismo nacional de normalización, según el Decreto 2269 de 1993. La norma NTC-ISO-IEC 27001 (Primera actualización) fue ratificada por el Consejo Directivo de 2013-12-11. (Icontec, 2013)

Sin embargo la evolución histórica de la familia ISO 27000 presenta aproximadamente 29 normas, donde para la presente investigación vale la pena resaltar la norma ISO/IEC 27005 la cual 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. Es la más relacionada a la actual British Standard BS 7799 parte 3. Publicada en junio de 2008. Revisada en junio de 2011. (ISO 27001, 2013)

2.1.1 Antecedentes. De acuerdo al marco de esta investigación, los antecedentes constituyen una serie de documentos académicos donde se han realizado estudios aplicados a diferentes organizaciones en referencia a la gestión de riesgos de la información, a continuación se referencian aquellos que más se asocian al objetivo general presentado para este trabajo de grado.

A nivel internacional la tesis de (Calderón, 2015) Análisis de Riesgos Informáticos y Desarrollo de un Plan de Seguridad de la Información para el Gobierno Autónomo Descentralizado Municipal de Catamayo, presenta un diseño del Plan de Seguridad de la información, el cual se desarrolló con base a la etapa planificar de la Norma ISO 27001, y se

consideraron las recomendaciones proporcionadas en la Norma ISO 27002. El punto de partida para el diseño fue la identificación de los activos que contribuyen a la entrega de los servicios a los usuarios, además de las medidas de seguridad implementadas en la institución, finalmente se realizó un análisis de riesgos, identificando los activos críticos, así como las amenazas a las que están expuestos dichos activos y creando perfiles de riesgo para cada activo critico incluyendo el impacto, la probabilidad de ocurrencia de amenazas y el plan para el tratamiento del riesgo. Esta tesis se articula por que plantea una metodología para hacer el análisis de riesgos y se basa en la etapa de planificación uno de los objetivos de este proyecto.

Por otra parte (Cavalcanti, 2012), presenta su título Sistema para el Análisis y Gestión de Riesgos, donde busca establecer el proceso para la identificación, análisis, evaluación y tratamiento de riesgos, considerando la seguridad de la información del negocio, los requisitos legales y reglamentarios para así poder agilizar la toma de decisiones por parte de la gerencia de proyectos, realizando un adecuado seguimiento y control de riesgos que evite un impacto negativo en los objetivos de la organización. Finalmente busca desarrollar un sistema para mejorar los procesos de gestión de riesgos, obteniendo resultados positivos para el aseguramiento de la información. En este sentido se articula desde los objetivos específicos estableciendo las etapas del desarrollo de la gestión del riesgo.

A nivel nacional, (Garavito, 2015) con su trabajo Análisis Y Gestión Del Riesgo De La Información En Los Sistemas De Información Misionales De Una Entidad Del Estado, Enfocado En Un Sistema De Seguridad De La Información, plantea como objetivo realizar un análisis de seguridad informática para determinar, y gestionar los posibles riesgos de la entidad enfocados

en su Sistemas de Información Misional, en coherencia con la presente propuesta se pudo establecer que la entidad estatal para la cual se realizó el análisis y gestión del riesgo está encargada de coordinar, asesorar y ejecutar con otras entidades públicas y privadas a personas de un grupo específico de la sociedad.

(Nieves, 2017) en el documento Diseño De Un Sistema De Gestión De La Seguridad De La Información (SGSI) Basados En La Norma ISO/IEC 27001:2013, presenta una guía, que permitirá evaluar la integridad, confidencialidad y disponibilidad de los activos (Hardware - Software) de información a las oficinas de Ingreso de Centros de Educación Técnica y Tecnológica del Cesar. Para el desarrollo de lo anterior, se dividió en tres fases: Planeación, incluyó un análisis de situación y descripción de los procesos, en la fase de Preparación incluyó GAP análisis, activos de información (análisis y evaluación de riesgos), y la última fase Capacitación y sensibilización, en donde se involucra la concientización de seguridad de sistemas y activos de información.

(Molano, 2017), en su trabajo Proyecto De Investigación Estrategia Para Implementar Un Sistema De Gestión De La Seguridad De La información Basada En La Norma ISO 27001 En El Área De Ti Para La Empresa Market Mix, se enfocó en implementar una estrategia de un sistema de gestión de la seguridad de la información basadas en la norma ISO 27001 que permitió identificar los riesgos o vulnerabilidades que amenazan la empresa Market MX obteniendo al final un diagnóstico del estado actual de la empresa Market mix, y así poder emitir las recomendaciones que deben estar acorde a la normatividad vigente. Aunque en la literatura se puede encontrar múltiples investigaciones, la anterior selección de trabajos de grado, permite

evidenciar la importancia de la aplicación de las metodologías de la gestión de riesgos en cuanto a seguridad de la información, genera resultados y conclusiones respecto a las posibles consecuencias de la materialización de los mismos y exponen diferentes metodologías para la administración del riesgo.

2.2 Marco Conceptual

En principio definiremos Riesgo en la seguridad de la información, como aquel potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. Se mide en términos de una combinación de la probabilidad de que suceda un evento y sus consecuencias. (Norma Técnica NTC-ISO/IEC 27005, 2013). En este sentido el proceso de gestión de riesgo en la seguridad de la información se definirá, como consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento:

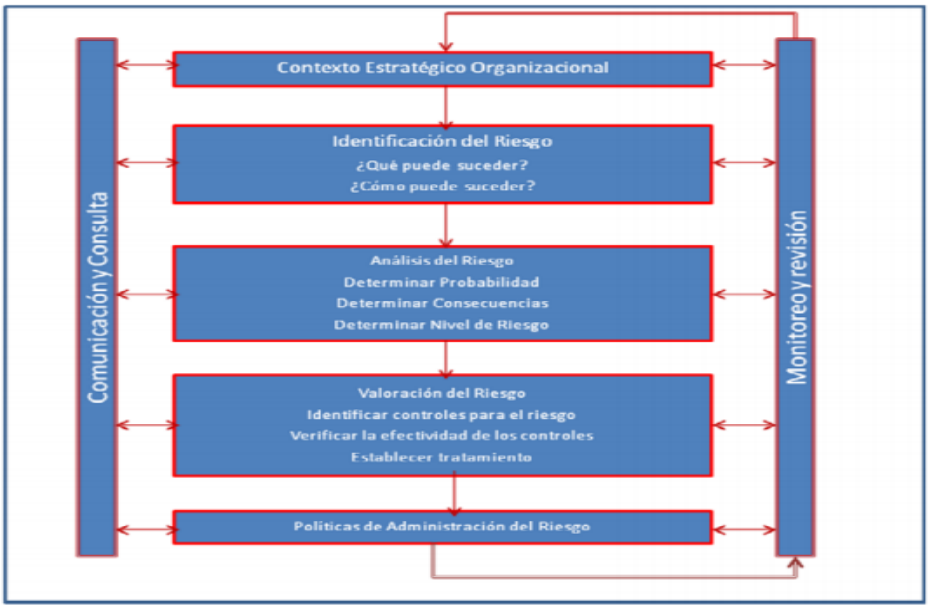

Figura 2. Proceso de administración del riesgo. Fuente: Tomado de la Cartilla de Administración de Riesgos del DAFP

A partir de esto conceptualizaremos los siguientes términos, Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo. (Norma Técnica NTC-ISO/IEC 27005, 2013)

Análisis de riesgo. Uso sistemático de la información para identificar las fuentes y estimar el riesgo. (Norma Técnica NTC-ISO/IEC 27005, 2013)

Valoración del riesgo. Proceso global de análisis y evaluación del riesgo. (Norma Técnica NTC-ISO/IEC 27005, 2013)

Por otra parte, se definirá que la Política de Administración del Riesgo es aquella expresión documentada que establece el marco de referencia para fijar objetivos y establezca un sentido general de dirección y principios para la acción con relación a la seguridad de la información. (Norma Técnica NTC-ISO/IEC 27005, 2013)

2.3 Marco Contextual

D.R.G TOTAL SERVICIOS ENERGY S.A.S es una firma de profesionales especializados en consultoría jurídica y gestión de proyectos, ubicada en la ciudad de Aguachica Cesar y sede en Bogotá D.C. con alrededor de 10 empleados, que cuenta con los conocimientos y la experiencia para asesorar y asistir a empresas y clientes en áreas del Derecho como la administrativa, ambiental, minera, petrolera, laboral, tributaria, corporativa, hidrocarburos y comercial.

Actualmente la empresa no cuenta con un sistema de gestión de información, por lo cual no ha realizado ningún tipo de gestión del riesgo, sin embargo ha determinado la descripción de su operación así:

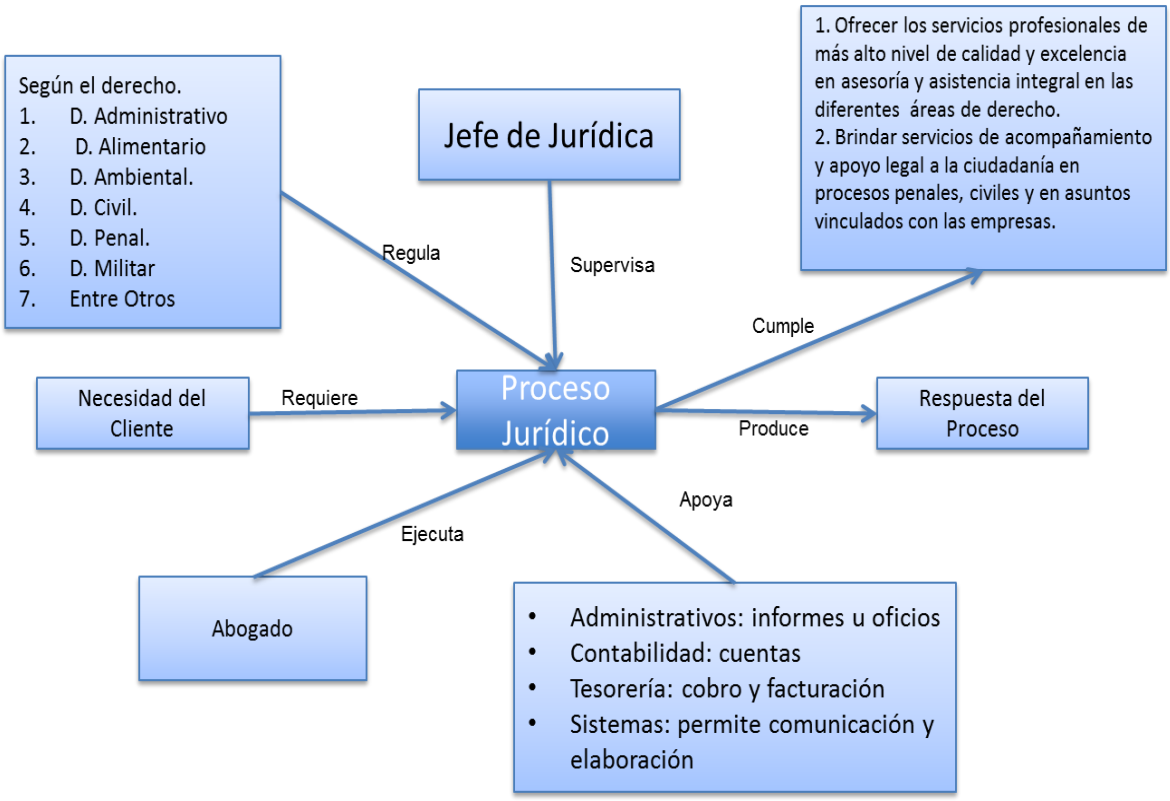

Figura* 3. *Descripción de procesos D.R.G. Fuente: Empresa D.RG (2018)

En cuanto a infraestructura física y tecnológica para el manejo de la información, la empresa cuenta con un computador central, desde donde se realizan los procesos administrativos y computadores personales de cada Abogado que presta servicios en cada caso. La información física impresa, se maneja en un archivo dentro de la misma oficina. Ver Anexos 1 (Fotos). La empresa no maneja sistemas de información, pero si hace uso de elementos office como hojas de cálculo, procesadores de texto, entre otros.

2.4 Marco Teórico

Desde los principios de la humanidad, el hombre ha generado y procesado información, a raíz de esto ha evolucionado social, cultural, económica y tecnológicamente. De igual manera, el desarrollo económico nace a partir de la definición de Empresa, como aquella que aúna el trabajo y el capital para generar un bien o servicio. En este sentido, las teorías de la administración definen que en las organizaciones se administran personas o cosas,

El éxito de toda función social y en particular, de las que realizan en una empresa, depende de dos elementos distintos: las personas que las llevan a cabo y las dirigen, y las cosas o bienes de que se valen como instrumentos para realizarlas. (Reyes, 1992, pág. 45)

Si bien esta teoría parece aun darse en las empresas, la administración moderna incluye un elemento más dentro de la ecuación, este elemento es la información, sin embargo la forma en que esta se administra, es diferente a como se administran los recursos tradicionales de una empresa. (Pablos, 2006).

El mismo de (Pablos, 2006) plantea que, Uno de los principales problemas con los que se enfrentan las organizaciones actuales y sus dirigentes es el exceso de información. Hoy nos llega y podemos acceder a más información que nunca. Se estima que en los últimos 50 años la humanidad ha producido más información que en toda su historia anterior y que en estos momentos cada 4 años se duplica en el mundo la información existente. p.34.

Podríamos entonces analizar que existe una relación directa entre el éxito de la empresa y la administración de su información. Esta administración se da de muchas maneras y actualmente se puede gestionar por medio de la informática.

La informática es una ciencia que se ocupa del tratamiento automático de la información usando equipos electrónicos llamados computadores. El tratamiento de la información consta de tres fases: la entrada de datos, el procesamiento de dichos datos, los cuales se convierten en información y la salida de los resultados. (Segunda Cohorte Doctorado en Seguridad Estratégica, 2014, pág. 11)

Si retomamos la teoría sobre que en las empresas modernas existe demasiada información y que la informática es una herramienta para administrarla, debemos formularnos la pregunta en cómo proteger esa información que está siendo tratada por medios informáticos, de ahí llegamos al planteamiento de la seguridad de la información. Analizamos este concepto desde la Norma ISO 27001:2013, como aquel que se encarga de la preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.

(Areitio, 2008) propone el siguiente postulado, La meta final de la seguridad es permitir que una organización cumpla con todos sus objetivos de negocio o misión, implementado sistemas que tengan un especial cuidado y consideración hacia los riesgos relativos a las tics de la organización, a sus socios comerciales, clientes, administración pública, suministradores, etc. p.2

Más adelante plantea que los servicios de seguridad permiten implementar políticas de seguridad en una organización. Se establecen en los sistemas de información formados por redes, computadores, personas, etc. Con objeto de dar protección a todas las entidades identificables. p.11

Con todo lo anterior definimos que la información es un recurso más dentro de las empresas, que es considerado dentro de la administración moderna, así mismo requiere un tratamiento especial por su importancia para la generación de valor, para lo cual se usa la informática, y que por esto demanda de una seguridad. Esta seguridad se puede organizar por medio de políticas y sistemas de información. Ahora bien, cuando se habla de un sistema de seguridad de la información, hablamos de parte del sistema de gestión global, basado en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información. (ISO 27001, 2013)

Sullivan (2016) expone que la gestión de riesgos de seguridad de la información es el proceso de identificar, comprender, evaluar y mitigar los riesgos –y sus vulnerabilidades subyacentes– y el impacto en la información, los sistemas de información y las organizaciones que dependen de la información para sus operaciones. Además de identificar los riesgos y las medidas de mitigación del riesgo, un método y proceso de gestión del riesgo ayudará a:

Identificar los activos críticos de información. Un programa de gestión de riesgos puede ampliarse para identificar también a personas críticas, procesos de negocio y tecnología.

Comprender por qué los activos críticos escogidos son necesarios para las operaciones, la realización de la misión y la continuidad de las operaciones. Para cumplir con la gestión de riesgos como componente de preparación para la ciberseguridad, una organización debe crear un sólido programa de evaluación y gestión del riesgo de la seguridad de la información. Si ya existe un programa de gestión del riesgo empresarial (ERM), un programa de gestión de riesgos de seguridad de la información puede soportar el proceso de ERM.

Esto incluye entonces dentro de la administración de las empresas, la gestión de riesgos de la información como un proceso natural de la cadena de valor empresarial. “Dependiendo del alcance y los objetivos de la gestión del riesgo, se pueden aplicar diferentes enfoques pero debe ser adecuado y que contenga criterios como: criterios de evaluación del riesgo, criterios de impacto, y criterios de aceptación del riesgo”. (Mintic., 2016, pág. 14)

Por otra parte, el análisis de riesgos introduce un enfoque riguroso y consecuente para la investigación de factores que contribuyen a los riesgos. En general implica la evaluación del impacto que una violación de la seguridad tendría en la empresa; señala los riesgos existentes, identificando las amenazas que afectan al sistema informático y la determinación de la vulnerabilidad del sistema a dichas amenazas…...la gestión de riesgos es un proceso separado que utiliza los resultados del análisis de riesgos para selección e implantar las medidas de seguridad adecuadas para controlar los riesgos identificados. (Pablos, 2006, pág. 180)

El tratamiento de los riesgos se basara entonces en la premisa establecida por (Mintic, 2016), como se puede observar en la tabla a continuación,

Tabla 1.
Etapa del tratamiento

Etapas	**Proceso De Gestión Del Riesgo En La Seguridad de La Información**
Planear	Establecer Contexto Valoración del Riesgo Planificación del Tratamiento del Riesgo Aceptación del Riesgo
Implementar	Implementación del Plan de Tratamiento de Riesgo
Gestionar	Monitoreo y Revisión Continuo de los Riesgos
Mejora Continua	Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información

Fuente: Mintic (2016)

¿Qué es el DAFP? El Departamento Administrativo de la Función Pública (DAFP) es la entidad técnica, estratégica y transversal del Gobierno Nacional que contribuye al bienestar de los colombianos mediante el mejoramiento continuo de la gestión de los servidores públicos y las instituciones en todo el territorio nacional. (Roncancio, 2018)

El DAFP hace parte de los 24 sectores que componen la Rama Ejecutiva Nacional, siendo cabeza del sector Función Pública, del cual también hace parte la Escuela Superior de Administración Pública (ESAP); entidad descentralizada de carácter universitario con presencia regional.

Los temas sobre los cuáles el DAFP trabaja se listan a continuación. En la imagen abajo se pueden ver en detalle.

- Empleo Público
- Gestión Pública
- Fortalecimiento Institucional

- Participación, Transparencia y Servicio al Ciudadano

2.5 Marco Legal

Se establecerá el marco legal sobre los tres conceptos principales de la investigación, Empresa, Información y Riesgos. A continuación se relacionan las principales normas relacionadas con la investigación:

Código de Comercio (Decreto 410 de 1971).

Artículo 1. Aplicabilidad de la ley comercial. Los comerciantes y los asuntos mercantiles se regirán por las disposiciones de la ley comercial, y los casos no regulados expresamente en ella serán decididos por analogía de sus normas.

Artículo 515. Definición de establecimiento de comercio. Se entiende por establecimiento de comercio un conjunto de bienes organizados por el empresario para realizar los fines de la empresa. Una misma persona podrá tener varios establecimientos de comercio, y, a su vez, un solo establecimiento de comercio podrá pertenecer a varias personas, y destinarse al desarrollo de diversas actividades comerciales

Ley 603 de 2000. Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

Ley estatutaria 1266 del 31 de diciembre de 2008. Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Ley 1273 del 5 de enero de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1341 del 30 de julio de 2009. Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

Ley estatutaria 1581 de 2012. Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.

Adicional se propone la adopción del Ministerio de Tecnologías de la Información y las Comunicaciones - Mintic quien a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones; publica El Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con

el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión. El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad será actualizando periódicamente; reuniendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información. (Mintic, 2016)

Capítulo 3. Diseño metodológico

3.1 Tipo De Investigación

De acuerdo al objetivo de la investigación, se propone la realización de una investigación de tipo descriptivo, Arias (1999) define que es "aquella que consiste en la caracterización de un hecho, fenómeno con el fin de establecer su estructura o comportamiento". p.20

Por otra parte Muñoz (2015) establece que:

En la investigación descriptiva el investigador diseña un proceso para descubrir las características o propiedades de determinados grupos, individuos o fenómenos; estas correlaciones le ayudan a determinar o describir comportamientos o atributos de las poblaciones, hechos o fenómenos investigados, sin dar una explicación causal de los mismos. (p. Sección 10)

En referencia al enfoque, se establece el cualitativo, el mismo (Muñoz, 2015) lo explica así:

La Investigación cualitativa se puede identificar como una investigación donde la recolección de datos no demanda su medición métrica. La indagatoria se centra en los hechos y su interpretación….la recolección de datos consiste en obtener perspectivas, apreciaciones, puntos de vista, prioridades e intereses de los participantes. (p. Sección 22)

3.2 Población

La población o universo a estudiar es el conjunto total de los objetos de estudio, (eventos, organizaciones, comunidades, personas) que comparten ciertas características comunes funcionales a la investigación, vale decir debemos definir sobre qué o quiénes se van a recolectar los datos, esto depende del enfoque elegido cualitativo cuantitativo mixto de planteamiento del problema investigar y de los alcances del estudio. (Gómez, 2006, pág. 109)

Para el caso de la investigación, la población se considera todos los procesos de la empresa D.R.G Total Servicios Energy S.A.S, los cuales son:

- Proceso jurídico
- Consultoría y asesoría
- Gestión de negocio
- Gestión administrativa
- Gestión humana
- Gestión de comunicaciones y de información

3.3 Muestra

La muestra debe ser, en esencia, un subgrupo representativo de la población…las características de las unidades de análisis definirán las características de la muestra. (Gómez, 2006, pág. 111).

Debido a que la empresa tiene definidos sus procesos, la muestra será igual a la población y se determinaran la información producida en la empresa para un año seleccionado, de acuerdo a la delimitación operativa.

3.4 Técnicas de recolección de la información

Para la recolección de información se utilizaran dos tipos de fuentes, primarias y secundarias.

Fuentes Primarias. Las fuentes primarias están constituidas por la documentación y registros producidos por la empresa, para lo cual se utilizara una lista de chequeo. Esta lista consta de columnas que permiten identificar el nombre del activo de información, clasificarlo según el tipo, determinar sus atributos, su ubicación, el propietario y el modo de acceso. Ver Anexo 2.

Fuentes Secundarias. Las fuentes secundarias están constituidas por la percepción de los empleados de la empresa, para lo cual se utilizara la técnica de la entrevista, “Las entrevistas se utilizan para recabar información en forma verbal, a través de preguntas que propone el analista” semiestructurada, en la que el entrevistador tiene libertad de hacer preguntas adicionales. (Bautista, 2003), entre otras herramientas de cuestionarios, listas de chequeo y demás que se consideren. Ver Anexo 3.

Debido a que la empresa se clasifica como Microempresa, pues su personal no supera las 10 personas (Ley 590, Fomento de la Micro, Pequeña y Mediana Empresa,) debido a que

actualmente cuenta con 5 personas y de acuerdo a su estructura se entrevistará a una persona por cada nivel, directivo, profesional y asistencial.

Capítulo 4. Resultados

4.1 Diagnóstico del estado actual de la empresa D.R.G TOTAL SERVICIOS ENERGY S.A.S frente a la gestión de riesgos asociados a la información.

4.1.1 Información General de la empresa D.R.G TOTAL SERVICIOS ENERGY S.A.S.

La misión de D.R.G TOTAL SERVICIOS ENERGY S.A.S. es la asesoría legal; cada trabajo se realiza buscando suplir las necesidades de los clientes y propendiendo exceder sus expectativas, para que bajo dicha asesoría se tomen las mejores decisiones.

Ahora bien, la empresa al prestar este tipo de servicios, es una organización que maneja información privada de cada cliente, como datos personales, legales y financieros. En este sentido, a continuación se relaciona las políticas corporativas de la empresa versus el análisis asociado con la seguridad de la información:

Tabla 2.
Análisis diagnóstico de la empresa D.R.G.

POLITICA CORPORATIVA	ANALISIS RESPECTO A LA SEGURIDAD DE LA INFORMACION
PRINCIPIOS Desde la formación personal y como profesionales, se ha desarrollado los principios en los que se basa D.R.G Total Servicios Energy S.A.S, El Respeto por nosotros mismos y por nuestros clientes es uno de los principales; siempre estamos buscando lo mejor para los clientes y nuestro personal, basados en los	Los principios de la empresa se fundamentan en el respeto por los clientes, esto sin duda debe articularse con la seguridad de la información tanto personal como jurídica, también exponen en el contexto a la competencia lo cual se relaciona con la capacidad de empresa de manejar información clasificada y/o privada.

valores que hemos construido en varios años de experiencia. Destacamos el Trabajo En Equipo y la Lealtad hacia nuestros valores y los compromisos adquiridos. Estamos comprometidos con cumplir la visión y misión de nuestra firma, entregando siempre lo mejor de nosotros mismos, llevando una sana Competencia que sea ejemplo para nuestros similares y que nos permita seguir siendo la mejor opción en asesorías jurídicas y gestión de negocios.	Sin embargo, como se puede observar en los principios de la empresa no se hace referencia a la información de manera explícita y adicionalmente no se cumple con el principio de responsabilidad de la dirección de la norma ISO 27001 donde se establece que se debe comunicar a la organización la importancia de cumplir los objetivos de seguridad de la información.
VALORES Honestidad: Nuestro actuar siempre está condicionado por la transparencia, comprendemos que los intereses colectivos priman sobre los intereses particulares al trabajar por alcanzar los objetivos de nuestros clientes. Conocimiento: Es nuestro mayor capital, nuestra política es fortalecer el capital intelectual de la empresa y aportar nuestros conocimientos para el favorecimiento de nuestros clientes y de la sociedad. Actualización: Somos conscientes que el mundo cambia a cada instante y que cada situación requiere de acciones propias, por lo tanto estamos siempre a la vanguardia, actualizándonos para estar preparados para cualquier reto que se nos presente en interés de nuestros clientes. Especialización: Cuando abordamos un caso, somos conscientes del valor del mismo y que estamos en capacidad de afrontarlo, somos especialistas en cada una de las ramas en las que ofrecemos nuestros servicios. Experiencia: Nuestro conocimiento no se limita a lo aprendido en un aula universitaria, también está formada por la acumulada al haber asumido innumerables retos como profesionales, lo que nos capacita para tomar las mejores decisiones en pro de nuestros clientes y nuestra firma.	Los valores se articulan con los requisitos de la ISO 27001 en cuanto a la definición de la seguridad de la información, pues de manera explícita se cita que para mantener segura la información se debe acudir a la confidencialidad e integridad que en este caso se relaciona con el valor de la honestidad. Los demás valores organizacionales responden a las propiedades de la información como trazabilidad, fiabilidad para el caso de la Especialización y Experiencia. Entonces de acuerdo con lo anterior se puede analizar que en el momento en que la empresa quiera iniciar con la implantación de un SIG puede articular el requisito de la norma ISO 27001 inciso 2.4.1 literal 3, que especifica a estos valores como contexto organizacional estratégico con la gestión del riesgo.
OBJETIVO ESTRATEGICO Consolidarnos como una empresa líder en la asesoría y apoyo de procesos legales con los	Los objetivos estratégicos también hacen parte del contexto organizacional, la

más altos estándares de eficiencia y eficacia y constituirnos como la mejor organización de tipo jurídico en la región. OBJETIVOS 1. Ofrecer los servicios profesionales de más alto nivel de calidad y excelencia en asesoría y asistencia integral en las diferentes áreas de derecho. 2. Asistir en representación de la empresa y/o persona en los procesos judiciales en calidad de actora o demandada. 3. Brindar servicios de acompañamiento y apoyo legal a la ciudadanía en procesos penales, civiles y en asuntos vinculados con las empresas. 4. Desarrollar proyectos de ordenanzas, reglamentos, estatutos y demás instrumentos de carácter legal relacionados con el funcionamiento de la empresa. 5. Elaborar reglamentos internos, normas, proyectos de ordenanzas y disposiciones legales de resoluciones administrativas de la institución.	expectativa de alcanzar el más alto nivel de calidad debe incluir entonces la seguridad de la información y en general desarrollar los fines propios de la empresa genera la capacidad para que la información sea eficaz, eficiente y oportuna. Sin embargo dentro de los objetivos estratégicos no se puede evidenciar la necesidad de garantizar los principios de la información que son veracidad y oportunidad. Ahora bien, es cierto que dentro de los documentos de carácter legal se enmarcan unas políticas ya establecidas para su resguardo, el objetivo relacionado con elaborar reglamentos internos, normas y proyectos debe articularse a la seguridad y gestión de riesgos de la información.

Fuente: DRGTOTAL, 2010 y los autores

También es necesario analizar la estructura organizacional de la empresa, pues nos permite identificar los factores críticos de éxito para la seguridad de la información, de acuerdo a los datos suministrados por la entidad, la empresa se ha constituido bajo una estructura jerárquica, como se muestra en la figura 4. La cual es la representación del organigrama, sin embargo en el momento de realizar la investigación es posible evidenciar que la operación real de la empresa no se da de acuerdo a dicha estructura, pues en realidad se está trabajando de acuerdo a una estructura por proyectos, es decir existe un nivel gerencial que es quien dicta las estrategias, un nivel operativo donde los abogados realizan los procesos de acuerdo a cada proyecto asignado y un nivel asistencial que da soporte a toda la operación, el cual radica en una sola persona.

Estructura organizacional

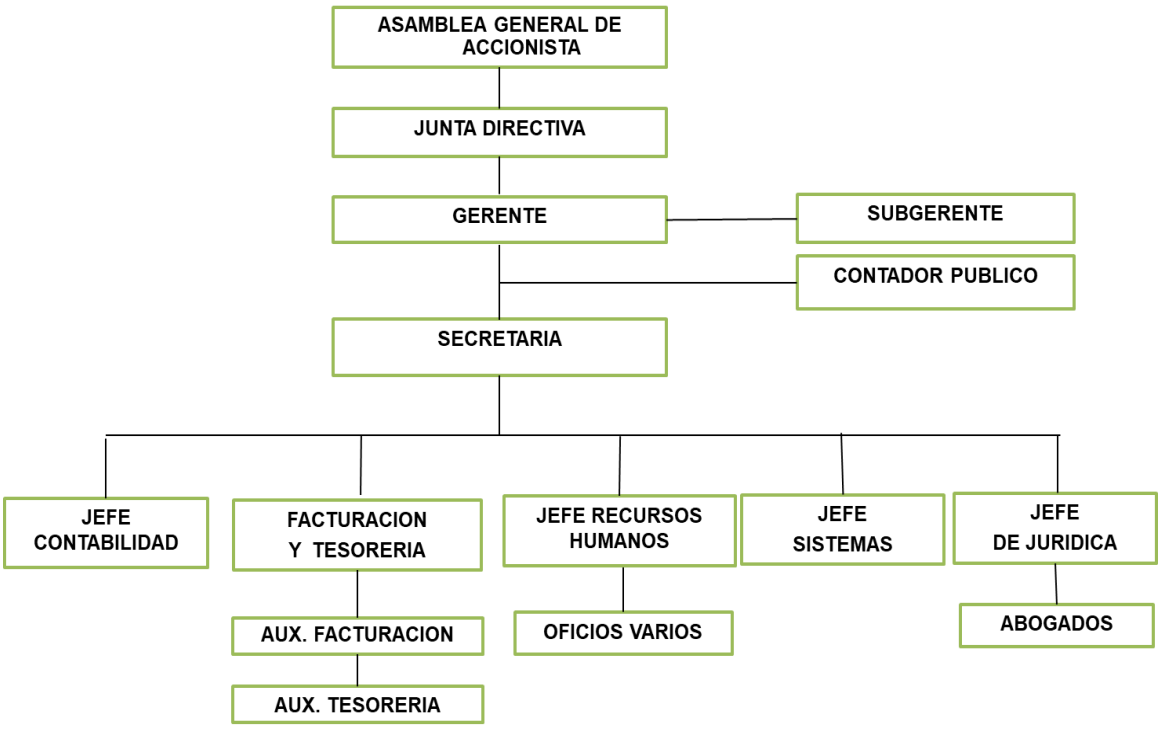

Figura 4. Estructura Organizacional D.R.G. Fuente: DRGTOTAL, 2010

Análisis del contexto organizacional. De acuerdo con la información organizacional se puede analizar que la empresa D.R.G es una empresa clasificada como microempresa por su número de empleados, la cual encarga varios procesos a una misma persona, el contexto general de la empresa, nos permite identificar que la seguridad de la información aun no hace parte de los objetivos, ni de las estrategias organizaciones de la empresa, pues aún no se encuentra manifiesta dentro de sus políticas corporativas. Por otra parte la estructura organizacional aunque está definida no se materializa tal cual como está planteada, sino que se asume por proyectos, condición que se tendrá en cuenta en la valoración del riesgo de la información.

4.1.2 Conocimiento del proceso de seguridad de la información en la empresa.

Para la empresa D.R.G TOTAL SERVICIOS ENERGY S.A.S aunque la información es la principal

entrada de sus procesos, aun no se ha definido un proceso de seguridad de la información, por lo tanto para determinar el estado de este concepto dentro de la entidad, se realizó una entrevista semiestructurada, que buscaba sondear con los tres niveles del recursos humano que se desempeñan, el nivel gerencial, profesional y asistencial, aspectos claves de la seguridad de la información dentro de la misma, de las diferentes entrevistas se presentan a continuación los resultados, así:

¿Cómo es el proceso de la seguridad en la información de la empresa D.R.G Total Servicios Energy S.A.S.? En los tres niveles entrevistados, se puso de manifiesto, la plena conciencia de que no existe un proceso de seguridad de la información, en todos los casos se expuso que la información de la empresa es la que se maneja en físico, por medio de un archivo llevado en carpetas y en digital donde los archivos se almacenan en el disco duro del computador principal, que se encuentra en la recepción de la empresa y que maneja la asistente.

¿A qué riesgos considera, se encuentra expuesta la información de la empresa D.R.G Total Servicios Energy S.A.S? Los entrevistados dieron a conocer por medio de sus respuestas que los riesgos identificados por, son básicamente el hurto de información y el daño de información, se manifestó que el computador es de acceso libre y por lo tanto no se cuenta con ninguna protección. De igual forma por las declaraciones se expresó que los abogados que llevan procesos manejan información en sus equipos personales por lo cual esa información que se genera dentro del proceso no está bajo control de cambios, ni control de integridad física. Otro factor importante es que la empresa no cuenta con dispositivos tecnológicos para prevenir los riesgos ya mencionados, es decir en general no existe seguridad de la información.

¿Cuáles son las herramientas que permiten proteger la información de la empresa D.R.G Total Servicios Energy S.A.S? La entrevista permitió conocer que no se conocen las herramientas de protección de información y ya que en todos los casos se habló de un antivirus del computador, también se identificó que la información que reconocen como desprotegida es la información de medios digitales, desconociendo la información física como algo que se deba proteger. Esta pregunta se articula con la anterior, pues los empleados no reconocen los tipos de información que se manejan en la empresa.

¿Cómo es el mantenimiento que se da a los equipos de cómputo de la empresa D.R.G Total Servicios Energy S.A.S? De manera generalizada, se reconoció que el mantenimiento se da por parte de un profesional en Ingeniería de Sistemas, pero que este no tiene una periodicidad, sino que es esporádico y reactivo. En las entrevistas se manifestó que no hay una función para hacer mantenimiento ni tampoco un contrato para este tipo de actividades.

¿Qué mejoramientos considera se podrían realizar en la empresa D.R.G Total Servicios Energy S.A.S para la seguridad de la información? Los tres niveles manifestaron que es necesario iniciar en la toma de acciones de mejoramiento para la seguridad de la información, las respuestas fueron muy dispersas, por lo que se puede analizar que no hay conocimiento previo del proceso. De igual forma expresaron que no se han realizado capacitaciones en el tema y que este sería un primer paso para abordar los mejoramientos que se necesitan en la empresa.

De manera general como primer resultado podemos identificar que la empresa D.R.G Total Servicios Energy S.A.S ha desarrollado unas políticas y estrategias para la calidad de su servicio de consultoría jurídica pero no ha determinado ni contemplado el proceso se seguridad de la información, de igual forma sus empleados no se encuentra capacitados en herramientas de seguridad de la información ni en gestión de riesgos de la información, los procesos y por ende los documentos y registros derivados de los mismos no se encuentran controlados ni asegurados, los equipos tecnológicos no cuentan con un proceso de mantenimiento, correctivo ni preventivo, las redes y demás canales de comunicación no se encuentran identificadas, por lo que se puede decir que la información de la empresa se encuentra desprotegida.

4.2 Proceso para la gestión del riesgo de la empresa D.R.G TOTAL SERVICIOS ENERGY S.A.S

Con el fin de contribuir a la esquematización de un proceso para la gestión del riesgo en la empresa D.R.G TOTAL SERVICIOS ENERGY S.A. y que se puedan identificar los factores críticos de éxito para inicialmente prevenir riesgos y en un futuro desarrollar acciones que les permitan implementar un sistema de seguridad de la información, se desarrolló en el marco de la norma ISO 27001:2013 la adaptación del proceso para la gestión de riesgos como propuesta a su futura implementación.

Para esto se inicia con adoptar el enfoque del P-H-V-A que define a los sistemas de gestión, luego se procede a caracterizar el proceso adaptado para la empresa, identificando las entradas, las salidas, los procesos de transformación, los registros y los responsables.

Tabla 3.
Proceso de gestión del riesgo de la información

	**CARACTERIZACIÓN DEL PROCESO GESTIÓN DEL RIESGO DE LA INFORMACIÓN**				
OBJETIVO	Identificar una metodología para la gestión del riesgo de la información de la empresa D.R.G Total Servicios Energy S.A con el fin de desarrollar criterios para la aceptación de los riesgos				
ALCANCE	Inicia con la identificación de los activos de información y termina con la selección de objetivos de control y tratamiento de riesgos. Aplica para los todos los activos de información.				
LÍDER DEL PROCESO	GERENCIAL	Gerente de la empresa			
REQUISITO ISO 27001	4.2.1 Establecimiento del SGSI, inciso d, e, y f				
PROVEEDOR	**ENTRADA**	**ETAPAS**	**PHVA**	**SALIDA**	**USUARIO**
Gerente, empleados, asistente, clientes	Información, equipos, conexión, redes	Identificación de los activos de información: Incluye realizar un inventario de todos lo que se considere un activo de información, que genere valor y deba ser protegido y conservado	P	Listado de activos de información de la empresa clasificados e identificados	Gerente, empleados, asistente, clientes
Gerente, empleados,	Listado de activos de	Identificación y valoración	H	Matriz de la identificación,	Gerente, empleados,

asistente, clientes	información de la empresa clasificados e identificados	de riesgos de información: Para realizar la valoración del riesgo se toma la metodología definida en la "Matriz de Calificación, Evaluación y respuesta a los Riesgos" expuesta en la "Guía de gestión de riesgos" (MINTIC, 2016. p 32)		calificación, evaluación y respuesta a los riesgos	asistente, clientes
Gerente, empleados, asistente, clientes	Matriz de la identificación, calificación, evaluación y respuesta a los riesgos	Tratamiento y control del riesgo: se toma la metodología definida en la "Guía de gestión de riesgos" (MINTIC, 2016. p 34)	V-A	Riesgos reclasificados de acuerdo a los controles vigentes	Gerente, empleados, asistente, clientes

Fuente .Autor del proyecto

4.2.1 Descripción de la metodología escogida. Para la identificación del riesgo el referente propone referir la probabilidad y el impacto de la acción denominada riesgo, esto permite hacer un cruce de información entre el impacto y la relación con su probabilidad de ocurrencia, así la empresa puede determinar que entre más raro e insignificante sea un riesgo se

encuentra más seguro, mientras en que si un riesgo es más probable y su impacto catastrófico se encuentra más expuesto.

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo *Moderada*: Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo *Alta*: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo *Extrema*: Reducir el riesgo, Evitar, Compartir o Transferir

Figura 5. Escalas de riesgo. Fuente: DAFP, 2010

La escala de valoración del riesgo por su parte permite identificar las acciones a tomar de acuerdo a la zona de riesgo que hayamos identificado, siendo esto que cuando se encuentra la empresa en la zona de riesgo baja, se puede asumir el riesgo sin prevenir que se materialice, en la zona moderada o se asume el riesgo o se reduce, en la zona alta es preciso que se evite, en dado caso se alcance a materializar se puede compartir puede ser con el cliente o transferir es decir no hacerse cargo del riesgo, finalmente la zona extrema su principal prioridad es reducir los impactos del riesgo.

4.3 Plan de gestión de riesgos de la empresa D.R.G TOTAL SERVICIOS ENERGY S.A.S

Con el fin de establecer el plan de gestión de riesgos de la información, para la empresa D.R.G TOTAL SERVICIOS ENERGY S.A.S, se toma como referente el capítulo 4.2 ESTABLECIMIENTO Y GESTIÓN DEL SGSI de la Norma ISO 27001:2013, donde se define a manera de propuesta los elementos sustanciales del contexto organizacional estratégico para la gestión del riesgo:

4.3.1 Política de seguridad de la información. D.R.G TOTAL SERVICIOS ENERGY S.A.S se compromete a tratar la información de sus clientes y la propia como su activo más importante, reconociendo la necesidad de la protección de los intereses que de ella se derive.

Es así, que de acuerdo al nivel de madurez de la empresa se establecerán acciones en búsqueda de fortalecer los principios de seguridad de la información, minimizar los riesgos y apoyarse en la innovación tecnológica.

Alcance de la política de seguridad de la información. Esta política alcanza a todos los procesos de la empresa D.R.G TOTAL SERVICIOS ENERGY S.A.S, así como a todo su recurso humano.

4.3.2 Objetivos de la seguridad de la información

- Mantener la confianza de sus clientes, socios y colaboradores

- Minimizar los riesgos operacionales en la gestión de la información
- Proteger la información privada de sus clientes, socios y colaboradores
- Proteger sus activos tecnológicos
- Garantizar la validez y oportunidad de la información
- Conservar la integridad de la información de sus clientes, socios y colaboradores

4.3.3 Principios y responsabilidades de la seguridad de la información.

La empresa D.R.G TOTAL SERVICIOS ENERGY adopta los principios de la Seguridad de Sistemas y Redes de Información, de acuerdo con la (NTC ISO27001:2013, p.33), los cuales serán:

- Toma de conciencia: Los sus clientes, socios y colaboradores deben estar conscientes de la necesidad de seguridad de los sistemas y redes de la información y de lo que pueden hacer para mejorar la seguridad.
- Responsabilidad: Todos los clientes, socios y colaboradores son responsables por la seguridad de los sistemas y redes de información.
- Respuesta: Se deberá actuar de una manera oportuna y en cooperación para evitar, detectar y responder ante incidentes de seguridad.
- Diseño e implementación de la seguridad: Se deberá incorporar la seguridad como un elemento esencial de los sistemas y redes de información.
- Gestión de la seguridad: Se deberá adoptar un enfoque amplio hacia la gestión de la seguridad

4.3.4 Definición del enfoque organizacional para la valoración del riesgo. De acuerdo a los principios organizacionales establecidos y en coherencia con el tipo de información generada y controlada dentro de la organización se adopta la metodología de gestión del riesgo definida por al MINTIC (2016), en la "Guía de gestión de riesgos" definido en el marco conceptual de la presente investigación, la cual se expone por medio de la etapa "Planear" donde se requiere de las siguientes actividades:

- Establecer Contexto
- Valoración del Riesgo
- Planificación del Tratamiento del Riesgo
- Aceptación del Riesgo

4.3.5 Identificación de activos de información. Dentro de la identificación de activo de información se pudo determinar los documentos y equipos asociados a los procesos de la empresa D.R.G TOTAL SERVICIOS ENERGY S.A.S, predominando dentro de ellos, que la información en su mayoría contiene datos personales (tanto naturales como jurídicos) de los clientes, los empleados y de la misma organización, así como que el 77% son susceptibles a fraudes o corrupción, entendiéndose por esto que son muy sensibles en cuanto a la veracidad de la información. Por otra parte el 100% de los documentos generados se soportan en medio físico y digital y tanto clientes como empleados tienen acceso a la información. Finalmente se identificaron 9 grandes activos de información dentro de la empresa Ver Tabla 2. Ellos son:

- Documentos legales de la empresa

- Minutas, proyectos
- Documentos legales de los clientes
- Cotizaciones, conceptos jurídicos
- Contratos, compras, oficios, actas de inicio y actas de entrega
- Equipos de cómputo
- Equipos de redes de internet
- Hojas de vida de los empleados
- Correos y comunicaciones, página web

Tabla 4

Inventario de activos de información

Lista de chequeo activos de información

EMPRESA: D.R.G Total Servicios Energy S.A.S.

Fecha: 8 de abril de 2019

Elaboró: AXEL ALONSO CARREÑO SUAREZ, JESSENIA ROMERO SAMPAYO

Revisó y aprobó: David Guillermo Ramos

A. Información del Activo						B. Atributos del Activo			C. Ubicación			D. Propiedad		E. Acceso	
Nº	Dependencia	Proceso/ Procedimiento	Código	Nombre	Descripción	¿El activo contiene datos personales?	¿El activo es susceptible de fraude o corrupción?	¿El activo es vital para la operación del proceso?	Física	Electrónica	Otro	Cliente	Empresa	Empleados	Clientes
1	Gerencia	Gestión de negocio	1	Documentos legales de la empresa	Incluye toda la documentación de la empresa	SI	SI	SI	X	X			x	x	
2	Abogados	Proceso jurídico	2	Minutas, proyectos	Son el producto de todos los procesos jurídicos adelantados por el	SI	SI	SI	X	X			X	X	X
3	Abogados	Consultoría y asesoría	3	Documentos legales de los clientes	Son los documentos legales entregados por el cliente a la empresa	SI	SI	SI	X	X		X		x	x
4	Abogados	Consultoría y asesoría	4	Cotizaciones, conceptos jurídicos	Son el producto de todos las asesorías adelantados por el	SI	SI	SI	s	s			s	s	s

6	5		4	
Comunicaciones	**Administrativa**		**Administrativa**	
Gestión de comunicaciones y de información	**Gestión humana**		**Gestión administrativa**	
9	**8**	**7**	**6**	**5**
Correos y comunicaciones, página web	**Hojas de vida de los empleados**	**Equipos de redes de internet**	**Equipos de computo**	**Contratos, compras, oficios, actas de inicio y actas de**
X	**SI**	**NO**	**NO**	**SI**
NO	**SI**	**SI**	**SI**	**SI**
NO	**NO**	**SI**	**SI**	**SI**
X	**x**			**X**
X	**x**			**X**
		X	**X**	
X	**x**	**X**	**X**	**X**
X	**x**	**X**	**X**	**X**

Fuente. Autor del proyecto

4.3.6 Identificación y valoración de riesgos de información. Con el fin de establecer un proceso para la gestión del riesgo, a continuación se presentan los resultados de la identificación y valoración de los riesgos, asociados a los activos de información de la empresa D.R.G TOTAL SERVICIOS ENERGY S.A.S.

Tabla 5.
Identificación y valoración de riesgos

Identificación de riesgos y Valoración de riesgos					
Activo de información	**Riesgo**	**Probabilidad**	**Impacto**	**Riesgo**	**Aceptación del riesgo**
Documentos legales de la empresa	Fuga de información al no tener bajo custodia los documentos	Bajo (1)	Medio (2)	2	Aceptable
Minutas, proyectos	Introducción de falsa información, en caso de que el abogado no se asegure de la veracidad de la información suministrada	Medio (2)	Bajo (1)	2	Aceptable
Cotizaciones, conceptos jurídicos	Alteración de la información en caso de que el gerente no se asegure de la veracidad de la información suministrada	Medio (2)	Alto (3)	6	Inaceptable
Documentos legales de los clientes	Corrupción de la información, en caso de que el cliente no suministre correctamente la información	Medio (2)	Alto (3)	6	Inaceptable
Hojas de vida de los empleados	Destrucción de información, en caso que no se lleve el debido control documental	Bajo (1)	Medio (2)	2	Aceptable
Contratos, compras, oficios, actas de inicio y actas de entrega	Degradación de los soportes de almacenamiento de la información, en caso de que no se haga mantenimiento al sitio de almacenamiento	Alto (3)	Alto (3)	9	Inaceptable
Equipos de redes de internet	Difusión de software dañino, en caso de que se descarguen software malintencionado o con virus	Bajo (1)	Alto (3)	3	Aceptable
Equipos de redes de internet	Errores de mantenimiento / actualización de programas (software), en caso que no se implemente un plan de mantenimiento	Medio (2)	Medio (2)	4	Tolerable
Equipos de computo	Errores de mantenimiento / actualización de equipos (hardware) en caso que no se implemente un plan de mantenimiento	Medio (2)	Medio (2)	4	Tolerable
Equipos de computo	Pérdida de equipos, en caso de descuido en las	Bajo (1)	Alto (3)	3	Aceptable

	instalaciones				
Equipos de computo	Abuso de privilegios de acceso a la información digital del computador principal	Bajo (1)	Medio (2)	2	Aceptable
Correos y comunicaciones, página web	Acceso no autorizado acceso a el computador principal sin autorización del gerente	Bajo (1)	Medio (2)	2	Aceptable
Correos y comunicaciones, página web	Errores de los usuarios en cuanto a seguridad de la información	Medio (2)	Bajo (1)	2	Aceptable
Equipos de computo	Robo de elementos físicos	Bajo (1)	Alto (3)	3	Aceptable

Fuente. Autor del proyecto

4.3.7 Valoración del riesgo. Dentro de las medidas para valorar los riesgos de información, se establecieron tres tipos de controles:

- Control preventivo: Asociado a los riesgos de la zona aceptable y toreable, este tipo de controles buscan prevenir la materialización del riesgo.
- Control correctivo y corrección: Asociado a la zona de riesgo inaceptable, este tipo de controles busca evitar el impacto del riesgo o establecer la medida una vez se materialice el riesgo.

La frecuencia de la aplicación de los riesgos se estableció en una escala permanente, mensual y semestral, esto con el fin de que una vez se identifiquen más riesgos y controles se apliquen en la misma medida de tiempo.

Finalmente, la nueva valoración arrojó que se pueden reducir los riesgos de manera sustancial, al aplicar controles correctivos y preventivos. La Tabla 6, muestra la valoración del riesgo residual después de valorados los controles.

Tabla 6.
Valoración del riesgo

Riesgo	Controles	Tipo de Control	Frecuencia	Responsable del Control	Afecta Probabilidad	Afecta Impacto	Riesgo Residual
Fuga de información al no tener bajo custodia los documentos	Restringir el acceso a la información	Preventivo	Permanente	Gerencia	1	1	1
Introducción de falsa información, en caso de que el abogado no se asegure de la veracidad de la información suministrada	Validación de la información	Preventivo	Permanente	Abogados	1	1	1
Alteración de la información en caso de que el gerente no se asegure de la veracidad de la información suministrada	Revisión de la información	Correctivo	Mensual	Abogados	1	3	3
Corrupción de la información, en caso de que el cliente no suministre correctamente la información	Contrastación de la información con su fuente original	Correctivo	Mensual	Abogados	1	3	3
Destrucción de información, en caso que no se lleve el debido control documental	Mantenimiento de archivos	Preventivo	Semestral	Abogados	1	1	1
Degradación de los soportes de almacenamiento de la información, en caso de que no se haga mantenimiento al sitio de almacenamiento	Mantenimiento del lugar de almacenamiento	Corrección	Semestral	Secretaria Administrativa	2	1	2
Difusión de software dañino, en caso de que se descarguen software malintencionado o con virus	Limitaciones en las descargas de internet	Preventivo	Permanente	Secretaria Administrativa	1	2	2

Errores de mantenimiento / actualización de programas (software), en caso que no se implemente un plan de mantenimiento	Ejecutar plan de mantenimiento	Correctivo	Mensual	Ingeniero de sistemas	1	1	1
Errores de mantenimiento / actualización de equipos (hardware) en caso que no se implemente un plan de mantenimiento	Ejecutar plan de mantenimiento	Correctivo	Semestral	Ingeniero de sistemas	1	1	1
Pérdida de equipos, en caso de descuido en las instalaciones	Identificación de inventario de equipos	Preventivo	Semestral	Secretaria Administrativa	1	2	2
Abuso de privilegios de acceso a la información digital del computador principal	Limitaciones de acceso por claves seguras	Preventivo	Permanente	Gerencia	1	1	1
Acceso no autorizado acceso a el computador principal sin autorización del gerente	Instalación de cámaras de seguridad	Preventivo	Permanente	Gerencia	1	1	1
Errores de los usuarios en cuanto a seguridad de la información	Capacitación	Preventivo	Semestral	Secretaria Administrativa	1	1	1
Robo de elementos físicos	Instalación de cámaras de seguridad	Preventivo	Permanente	Gerencia	1	2	2

Fuente. Autor del proyecto

Tabla 7.
Gestión del riesgo

Riesgo	Controles	Tipo de Control	Frecuencia	Actividad	Medio de verificación	Responsable de la actividad
Fuga de información al no tener bajo custodia los documentos, en las áreas de administración y jurídica.	Validación o Restricción para el acceso a la información tanto de cómputos, como física.	Preventivo	Permanente	Llevar un registro de quien y cuando se accede a la información legal de la empresa	Formato de seguimiento del control del riesgo. Ver Anexo 4.	Gerencia
Introducción de falsa información, en caso de que el abogado no se asegure de la veracidad de la información suministrada	Validación de la información	Preventivo	Permanente	Implementar procedimiento de aprobación de documentos donde se identifique quien elabora, quien revisa y quien aprueba	Formato de seguimiento del control del riesgo. Ver Anexo 4.	Abogados
Alteración de la información en caso de que el gerente no se asegure de la veracidad de la información suministrada	Revisión de la información	Correctivo	Mensual	Implementar procedimiento de aprobación de documentos donde se identifique quien elabora, quien revisa y quien aprueba	Formato de seguimiento del control del riesgo. Ver Anexo 4.	Abogados
Corrupción de la información, en caso de que el cliente no suministre correctamente la información	Contrastación de la información con su fuente original	Correctivo	Mensual	Implementar lista de chequeo de recepción de documentos de los clientes	Se propone Formato de seguimiento del control del riesgo. Ver Anexo 4.	Abogados

Destrucción de información, en caso que no se lleve el debido control documental	Mantenimiento de archivos	Preventivo	Semestral	Toda información que ya no relevante para la empresa se elimina, con el fin de mejorar la documentación de la empresa.	Se propone Formato de seguimiento del control del riesgo. Ver Anexo 4.	Abogados
Degradación de los soportes de almacenamiento de la información, en caso de que no se haga mantenimiento al sitio de almacenamiento	Mantenimiento del lugar de almacenamiento	Corrección	Semestral	Elaborar, implementar y mantener un plan de mantenimiento del archivo físico.	Se propone Formato de seguimiento del control del riesgo. Ver Anexo 4.	Secretaria Administrativa
Difusión de software dañino, en caso de que se descarguen software malintencionado o con virus	Limitaciones en las descargas de internet	Preventivo	Permanente	Elaborar, implementar y mantener un plan de mantenimiento de los equipos de cómputo.	Se propone Formato de seguimiento del control del riesgo. Ver Anexo 4.	Secretaria Administrativa
Errores de mantenimiento / actualización de programas (software), en caso que no se implemente un plan de mantenimiento	Ejecutar plan de mantenimiento	Correctivo	Mensual	Contratar mano de obra calificada de manera trimestral para hacer seguimiento al software utilizado en la oficina	Se propone Formato de seguimiento del control del riesgo. Ver Anexo 4.	Ingeniero de sistemas
Errores de mantenimiento / actualización de equipos	Ejecutar plan de mantenimiento	Correctivo	Semestral	Elaborar, implementar y	Se propone Formato de	Ingeniero de sistemas

(hardware) en caso que no se implemente un plan de mantenimiento				mantener un plan de mantenimiento de los equipos de cómputo.	seguimiento del control del riesgo. Ver Anexo 4.	
Pérdida de equipos, en caso de descuido en las instalaciones	Identificación de inventario de equipos	Preventivo	Semestral	Implementar un registro de inventario de equipos y mantener y actualizar el inventario de activos de información	Se propone Formato de seguimiento del control del riesgo. Ver Anexo 4.	Secretaria Administrativa
Abuso de privilegios de acceso a la información digital del computador principal	Limitaciones de acceso por claves seguras	Preventivo	Permanente	Implementar un sistema de claves de seguridad para los equipos de computo	Se propone Formato de seguimiento del control del riesgo. Ver Anexo 4.	Gerencia
Acceso no autorizado acceso a el computador principal sin autorización del gerente	Instalación de cámaras de seguridad	Preventivo	Permanente	Implementar un sistema de cámaras de seguridad y carnetizar a los empleados	Se propone Formato de seguimiento del control del riesgo. Ver Anexo 4.	Gerencia
Errores de los usuarios en cuanto a seguridad de la información	Capacitación	Preventivo	Semestral	Realizar dos capacitaciones al año en seguridad de la información a los empleados de la empresa	Se propone Formato de seguimiento del control del riesgo. Ver Anexo 4.	Secretaria Administrativa
Robo de elementos físicos	Instalación de cámaras de seguridad, sistema	Preventivo	Permanente	Implementar un sistema de cámaras de	Se propone Formato de seguimiento del	Gerencia

	de backup de información	seguridad y gestionar pólizas de seguro, así como realizar backup de la información	control del riesgo. Ver Anexo 4.

Fuente. Autor del proyecto

Capítulo 5. Conclusiones

De manera inicial se pudo establecer un marco de referencia para la gestión de riesgos basados en la norma NTC ISO 27001:2013, lo que permitió definir que es un riesgo, las características de los riesgos a nivel de la seguridad de la información y conocer diferentes aplicaciones que de acuerdo al estado del arte han evolucionado para entender la información como algo que va más allá de los documentos y trasciende a ser un activo organizacional.

El diagnóstico del estado actual de la empresa D.R.G TOTAL SERVICIOS ENERGY S.A.S frente a la gestión de riesgos asociados a la información, se puede ultimar aspectos relevantes como la necesidad de un plan de gestión de riesgos, pues no se contaba con ninguno y de la articulación de sus objetivos estratégicos y misionales, con la seguridad de sus activos de información.

Se formuló el proceso de administración del riegos, haciendo importantes avances en como las empresas, aunque sean micro, si pueden identificar entradas, etapas y salidas para hacer la gestión de sus riesgos de información.

El plan de gestión de riesgos permitió definir por medio de un inventario, donde se comprendió que los activos incluyen de manera sistémica, tanto información, como medios de soporte, como recurso humano. Una vez identificados dichos activos, se procedió a identificar los riesgos, que aunque muy evidentes en algunos casos, se van haciendo tan habituales que ya no se consideran peligrosos, lo que aumenta el impacto de su materialización.

Finalmente, la valoración de los riesgos implicó la propuesta de controles para el mejoramiento de algunos procesos y la integración de la política de seguridad de la información a las estrategias del negocio y por medio de esto, se podrá dar a conocer que es posible la aplicación de las teorías de la seguridad de la información, no solo en grandes empresas, sino también en pequeñas empresas, donde este puede ser el inicio de procesos de mejor calidad y mejor servicio.

Referencias

Advisiera Expert Solution Ltd. (2013). *¿Qué es la Norma ISO 27001?* . Obtenido de https://advisera.com/27001academy/es/que-es-iso-27001/

Areitio, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información.* Paraninfo.

Bautista, L. (2003). *La Entrevista.* Obtenido de http://data-collection-and-reports.blogspot.com/2009/05/la-entrevista.htm

Calderón, V. (2015). *Análisis de Riesgos Informáticos y Desarrollo de un Plan de Seguridad de la Información para el Gobierno Autónomo Descentralizado Municipal de Catamayo.* Ecuador: Ingeniería En Sistemas De La Universidad Nacional De Loja.

Cavalcanti, A. (2012). *Sistema para el Análisis y Gestión de Riesgos. Universidad Ricardo Palma Facultad de Ingeniería Escuela Profesional de Ingeniería Informática. Lima, Perú.* Obtenido de http://cybertesis.urp.edu.pe/bitstream/urp/36/1/cavalcanti_ad.pdf

Garavito, H. (. (2015). *Análisis Y Gestión Del Riesgo De La Información En Los Sistemas De Información Misionales De Una Entidad Del Estado, Enfocado En Un Sistema De Seguridad De La Información.* Bogotá: Universidad Abierta Y A Distancia Escuela De Ciencias Básicasv Escuela De Ciencias Básicas Tecnología E Ingeniería. Especialización En Seguridad Informática. . Obtenido de .

Gómez, M. (2006). *Introducción a la metodología de la investigación científica.* Brujas.

Icontec. (2013). *NORMA TÉCNICA NTC-ISO-IEC COLOMBIANA27001.* Bogota .

ISO 27001. (2013). TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). REQUISITOS.

Iso27000.es. (2013). *El portal de ISO 27001 en Español.* Obtenido de http://www.iso27000.es/,

Ladino, A. M., Villa, S. P., & López, E. A. (2011). *Fundamentos De ISO 27001 Y Su Aplicación En Las Empresas.* Scientia Et Technica.

Mintic. (2016). *Modelo de Seguridad.* Obtenido de https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

Mintic. (2016). *Guía de gestión de riesgos. Versión 3.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Molano, E. R. (2017). *Estrategia para implementar un sistema de gestión de laseguridad de la información basada en la norma ISO 27001.* Obtenido de https://repository.ucatolica.edu.co › bitstream › Esp Auditoria de sistemas

Muñoz, C. (2015). *Metodología de la investigación.* Oxford University Press.

Nieves, A. (2017). *Diseño De Un Sistema De Gestión De La Seguridad De La Información (SGSI) Basados En La Norma ISO/IEC 27001:2013. Institución Universitaria Politécnico Grancolombiano.* Facultad De Ingeniería Y Ciencias Básicas Especialización En Seguridad.

Norma Técnica NTC-ISO/IEC 27005. (2013). *Guía ISO/IEC 73:2002 Icontec.* Bogota.

Pablos, H. C. (2006). *Dirección y gestión de los sistemas de información en la empresa: una visión integradora. Biblioteca de Economía y Finanzas, Escuela Superior de Gestión Comercial y Marketing. Libros profesionales.* ESIC .

Pmg-ssi.com. (2013). *La NCh ISO 27001. Origen y evolución.* Obtenido de https://www.pmg-ssi.com/2013/08/la-nch-iso-27001-origen-y-evolucion/

Ponjuán, D. G. (2011). *La gestión de información y sus modelos representativos. Valoraciones.* Ciencias de la Información.

Reyes, A. (1992). *Administración moderna.* . Limusa.

Roncancio, G. (2018). *DAFP*. https://gestion.pensemos.com/que-es-el-dafp-y-cual-es-su-funcion-en-la-administracion-publica.

Segunda Cohorte Doctorado en Seguridad Estratégica. (2014). *Seguridad de la Información.* . Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica.

Apéndices

Apéndice A. Galería de fotos Empresa

Apéndice B. Lista de chequeo activos de información

Lista de chequeo activos de información
EMPRESA: D.R.G Total Servicios Energy S.A.S.

Fecha:
Elaboró:
Revisó y aprobó:

A. Información del Activo								B. Atributos del Activo			C. Ubicación			D. Propiedad		E. Acceso	
Nª	Dependencia	Proceso/ Procedimiento	Código	Nombre	Descripción	Observaciones	Tipo	¿El activo contiene datos personales?	¿El activo es susceptible de fraude o corrupción?	¿El activo es vital para la operación del proceso?	Física	Electrónica	Otro	Propietario	Empresa	Empleados	Clientes

Apéndice C. Entrevista percepción seguridad de la información

Entrevista percepción seguridad de la información
EMPRESA: D.R.G Total Servicios Energy S.A.S.

Fecha:

Nivel	**Directivo**		**Profesional**		**Asistencial**	

1. ¿Cómo es el proceso de la seguridad en la información de la empresa D.R.G Total Servicios Energy S.A.S.?

2. ¿A qué riesgos considera se encuentra expuesta la información de la empresa D.R.G Total Servicios Energy S.A.S?

3. ¿Cuáles son las herramientas que permiten proteger la información de la empresa D.R.G Total Servicios Energy S.A.S?

4. ¿Cómo es el mantenimiento que se da a los equipos de cómputo de la empresa D.R.G Total Servicios Energy S.A.S?

5. ¿Qué mejoramientos considera se podrían realizar en la empresa D.R.G Total Servicios Energy S.A.S para la seguridad de la información?

Nota: En la entrevista semiestructura se pueden añadir cuestionamientos para ampliar la información.

Se realizaron ocho entrevistas de las cuales se concluyeron:

En los tres niveles entrevistados, se puso de manifiesto, la plena conciencia de que no existe un proceso de seguridad de la información, en todos los casos se expuso que la información de la empresa es la que se maneja en físico, por medio de un archivo llevado en carpetas y en digital donde los archivos se almacenan en el disco duro del computador principal, que se encuentra en la recepción de la empresa y que maneja la asistente.

Los entrevistados dieron a conocer por medio de sus respuestas que los riesgos identificados por, son básicamente el hurto de información y el daño de información, se manifestó que el computador es de acceso libre y por lo tanto no se cuenta con ninguna protección.

La entrevista permitió conocer que no se conocen las herramientas de protección de información y ya que en todos los casos se habló de un antivirus del computador, también se identificó que la información que reconocen como desprotegida es la información de medios digitales, desconociendo la información física como algo que se deba proteger.

De manera generalizada, se reconoció que el mantenimiento se da por parte de un profesional en Ingeniería de Sistemas, pero que este no tiene una periodicidad, sino que es esporádico y reactivo. En las entrevistas se manifestó que no hay una función para hacer mantenimiento ni tampoco un contrato para este tipo de actividades.

Los tres niveles manifestaron que es necesario iniciar en la toma de acciones de mejoramiento para la seguridad de la información, las respuestas fueron muy dispersas, por lo que se puede analizar que no hay conocimiento previo del proceso.

La entrevista permitió conocer que no se conocen las herramientas de protección de información y ya que en todos los casos se habló de un antivirus del computador, también se identificó que la información que reconocen como desprotegida es la información de medios digitales, desconociendo la información física como algo que se deba proteger.

Apéndice D. Formato de seguimiento del control del riesgo

Monitoreo y revisión de los controles Formato de seguimiento del control del riesgo EMPRESA: D.R.G Total Servicios Energy S.A.S.							
Fecha	**Riesgo**	**Control**	**Efectividad de los controles**		**Evidencias y registros**	**Responsable**	**% cumplimiento**
			Se aplica	**No se aplica**			