UNIVERSIDAD SANTO TOMÁS
PRIMER CLAUSTRO UNIVERSITARIO DE COLOMBIA
MEDELLÍN

# Informe de Práctica Profesional

**Propuesta presentada a:**

**Universidad Santo Tomás-Sede Medellín**

**Primer Claustro Universitario de Colombia**

**Elaborado por:**

**Laura Román Calderón**
**Estudiante, Ingeniería de Telecomunicaciones**

**Enero de 2018**
**Medellín**

**Tabla de Contenido**

## Introducción

En este informe se presenta el proyecto de práctica que se realizó durante el segundo semestre del año 2017, cuyo propósito fue hacer una implantación del modelo de seguridad en información para ISAGEN.

> La pérdida de información sensible puede producirse accidental o malintencionadamente, pero, en cualquier caso, puede y suele acarrear un daño económico y de prestigio, afectando a la empresa y entidades asociadas a ella. Además, se debe tener en cuenta que cada vez más cantidad de información está en formato electrónico, y como profesionales del sector de las TI y en concreto de la Seguridad de la Información, la misión fundamental es protegerla. (Berciano, s.f)

Por lo tanto, una empresa de energía como ISAGEN requiere siempre estar fortaleciéndose en materia de seguridad, para dar continuidad al negocio y eficiencia en la prestación de servicios. Lo cual es muy importante porque continuamente en el proceso de aprendizaje se muestra que la confidencialidad, integridad y disponibilidad de la información es materia clave para la estabilidad de una institución.

## Resumen Ejecutivo

ISAGEN S.A. E.S.P es una empresa de generación y comercialización de energía concebida como un grupo humano que busca satisfacer las necesidades de otros grupos humanos, y construir con ellos bienestar y desarrollo para el país. Su gestión se desarrolla con los más altos estándares éticos, con responsabilidad social y ambiental, con sentido económico y orientación al cliente. (ISAGEN, s.f.)

Durante el transcurso de la práctica en esta empresa, fui parte de la Gerencia TIC en el grupo de Gestión de la Información y desde allí participé en la ejecución del plan de comunicaciones y materiales de comunicación sobre seguridad en información administrativa y de sistemas de Control Industrial (ICS), realicé un análisis de brecha frente a las normas ISO 27000 versión 2013, participé en el proyecto de implantación de la seguridad para sistemas de control industrial, entre otras cosas.

## Breve Descripción de la Empresa

La información que se suministrará a continuación fue sacada directamente de la página de ISAGEN www.isagen.com.co/SitioWeb/es/, desde allí se da clic en “Nosotros”. (Desde Nombre o razón social hasta Estructura Organizacional de ISAGEN)

**Nombre o razón social:** ISAGEN S.A E.S.P.

**Objeto social:** ISAGEN es una empresa de servicios públicos privada que tiene por objeto principal la generación y comercialización de energía eléctrica, la comercialización de gas natural por redes, así como la comercialización de carbón, vapor y otros energéticos.

**Equipo de trabajo:** Gerencia TIC.

**Área de desempeño:** Gestión de la Información.

**Misión de la empresa:** ISAGEN desarrolla proyectos de generación, produce y comercializa energía eléctrica y ofrece soluciones asociadas para satisfacer las necesidades energéticas de sus clientes y crear valor empresarial. La gestión se desarrolla con los más altos estándares éticos, con responsabilidad social y ambiental, con sentido económico y orientación al cliente.

**Propósito superior:** ISAGEN genera energía eficiente que contribuye a la mitigación del cambio climático, manteniendo la competitividad de la empresa en la industria, utilizando redes colaborativas y prácticas coherentes con el desarrollo humano sostenible y generando valor compartido con los grupos de interés.

**Pensamiento estratégico:** ISAGEN entrega energía confiable y limpia que contribuye a la productividad de sus clientes y a la satisfacción de la demanda para el desarrollo del país.

**Valores:** Los valores corporativos son los atributos y las actitudes que caracterizan a ISAGEN como Empresa y definen la forma como se asume el trabajo para entregar sus productos y servicios a quienes lo requieren, convirtiéndose en una empresa diferente en el mercado.

**Ética como valor fundamental:** Se concibe la ética como hacer las cosas correctamente y de buena fe, ser coherentes entre lo que se piensa, dice y hace, y privilegiar el bien común sobre el particular, contribuyendo a la sostenibilidad de la sociedad y del medio en que esta se desarrolla. Los valores con los que nos relacionamos con el entorno y buscamos nuestro crecimiento colectivo e individual son:

- Responsabilidad social y ambiental.
- Respeto a las personas.
- Disposición al cambio.
- Enfoque al cliente.
- Trabajo en equipo.
- Humildad.
- Sentido económico.
- Autocontrol.

**Estructura Organizacional de ISAGEN:**

Para desarrollar el trabajo, precisar responsabilidades, organizar recursos y lograr resultados productivos, configuramos gerencias. Cada proceso es asignado a una gerencia que depende directamente de la Gerencia General y que se configura a su vez en equipos y grupos de trabajo para responder por los asuntos de trabajo del proceso.

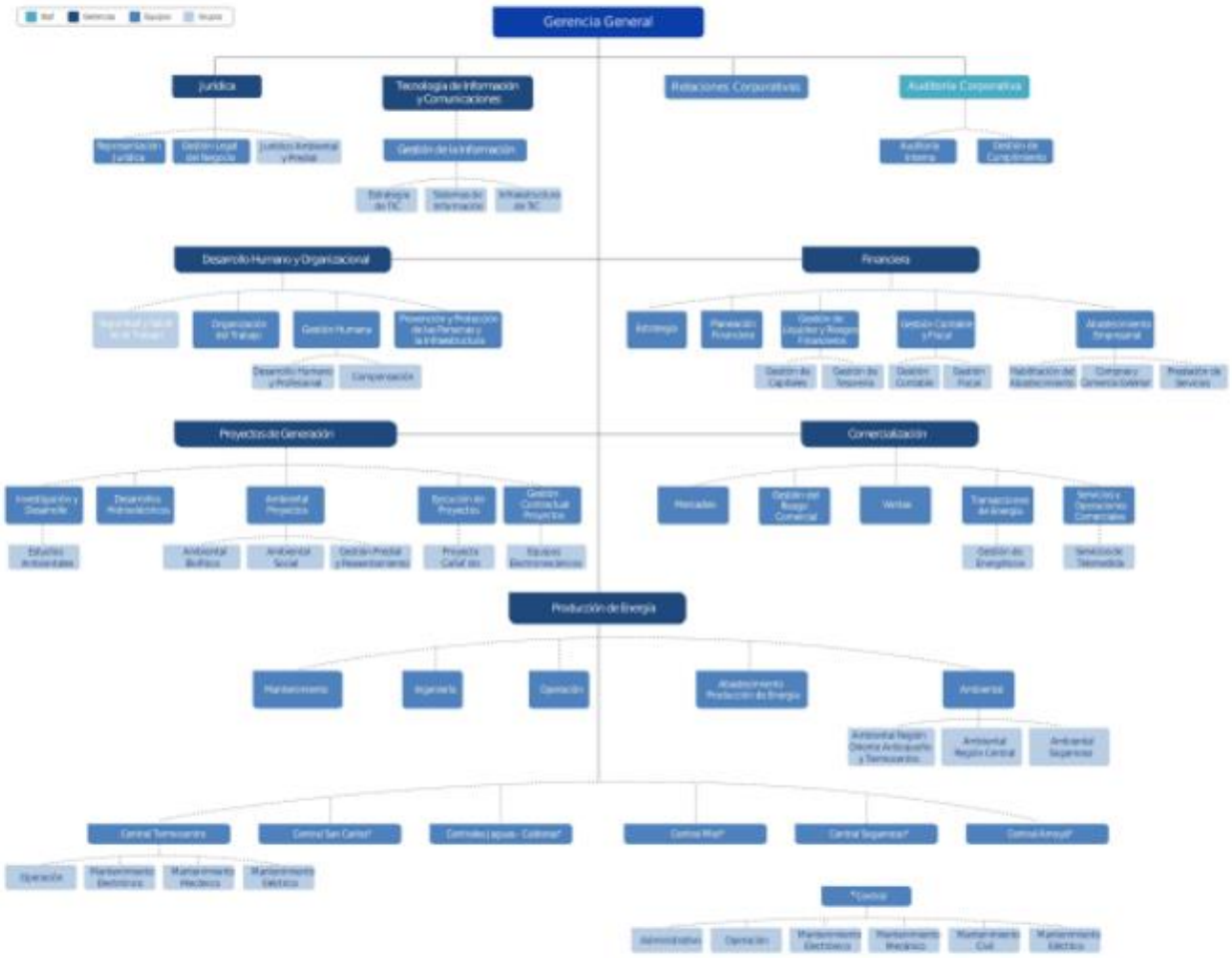


**Figura 1.** Estructura Organizacional de ISAGEN, elaborado por ISAGEN (2018).

# Propuesta de Trabajo

## Planteamiento del Problema

¿El trabajo elaborado como practicante en el área de seguridad de la información en una empresa como ISAGEN, permitirá que se logre todos los objetivos claves que ayuden a mantener la estabilidad en un área tan significativa para la empresa? ISAGEN por medio de diversos mecanismos busca estabilidad y un continuo crecimiento, teniendo como ejemplo de ello el uso de la ciberseguridad, una rama muy importante que busca estrategias para mantener la sostenibilidad en su modelo de negocio, protegiendo de eta manera sus activos de información (Un Activo de Información para ISAGEN es la información clave que se necesita para cumplir con los objetivos de trabajo y soportar la toma de decisiones en una empresa) a través de una serie de metodologías y procesos que garanticen el bienestar para la empresa.

ISAGEN cuenta con una infraestructura robusta, que debe estar constantemente vigilada para evitar que entes externos logren desestabilizarla, esto se menciona porque con el transcurso del tiempo ha evolucionado los métodos de ciberataques, es decir, la manera como hackers intentan entrar a las organizaciones para robar o secuestrar información valiosa a cambio de dinero, o simplemente para ocasionar algún daño.

Un caso particular es el Phishing Dirigido, el cual se centra en un grupo u organización donde por lo general sabe algunas cosas sobre la entidad que abordará, enviando un correo electrónico que utiliza información personalizada haciendo referencia a un amigo o a algún tipo de actividad online reciente que se haya llevado a cabo. Al dar la apariencia de provenir de alguien

que se conoce o de una entidad confiable, es más probable que se baje la guardia y se entregue la información que los estafadores están buscando. (Díaz Hernández , 2015)

Por tal motivo, se requiere de una serie de actividades para contrarrestar este tipo de eventualidades, por lo que el trabajo del estudiante en práctica es significativo para llegar a cumplir con los objetivos establecidos en la empresa.

**Justificación**

La empresa cuenta con un modelo de seguridad que brinda documentación clave para garantizar la integridad, disponibilidad y confidencialidad de la información. Así que se debe realizar una serie de actividades para seguir respondiendo con las necesidades que requiere ISAGEN, logrando de esta manera los propósitos establecidos para la práctica realizadas en el segundo semestre del año 2017.

**Plan de Trabajo – Desarrollo Práctica Profesional**

## Objetivo General

Buscar que la información cumpla con los criterios de confidencialidad, disponibilidad e integridad necesarios. Para ello, se requiere de un estudiante en práctica que aporte con sus ideas y conocimientos a la elaboración de las estrategias, estudios y procedimientos requeridos para llevar a cabo los proyectos.

## Objetivos Específicos

- Realizar un análisis de brecha frente a las normas ISO 27000 versión 2013.
- Diseñar Casos de uso que permitan realizar medidas de monitoreo para los principales activos y ciberactivos de la empresa.
- Participación en la incorporación de controles relacionados con el modelo de seguridad en información.
- Aportar en la revisión de cumplimiento de controles para el cumplimiento de la ley SOX
- Participar en la ejecución del plan de comunicaciones y materiales de comunicación sobre seguridad en información administrativa y de sistemas de Control Industrial (ICS)
- Participar en el proyecto de implantación de la seguridad para sistemas de control industrial.

**Cronograma de trabajo- Fases/Actividades y sus respectivos tiempos**

| ACTIVIDADES | MESES DE REALIZACIÓN DE LA PRÁCTICA PROFESIONAL (Julio 2017 a Enero 2018) | | | | | | |
|---|---|---|---|---|---|---|---|
| | Jul. | Ago. | Sep. | Oct. | Nov. | Dic. | Ene. |
| Realizar un análisis de brecha frente a las normas ISO 27000 versión 2013. | 0% | 0% | 5% | 10% | 80% | 100% | 100% |
| Participación en la incorporación de controles relacionados con el modelo de seguridad en información. | 100% | 100% | 100% | 100% | 100% | 100% | 100% |
| Aportar en la revisión de cumplimiento de controles para el cumplimiento de la ley SOX | 0% | 0% | 10% | 20% | 90% | 100% | 100% |
| Participar en la ejecución del plan de comunicaciones y materiales de comunicación sobre seguridad en información administrativa y de sistemas de Control Industrial (ICS) | 100% | 100% | 100% | 100% | 100% | 100% | 100% |
| Participar en el proyecto de implantación de la seguridad para sistemas de control industrial. | 5% | 10% | 30% | 50% | 80% | 100% | 100% |
| Capacitaciones a los trabajadores de ISAGEN para el uso de una herramienta que les permite manejar de una forma más sencilla los activos de información de la empresa. | 10% | 30% | 100% | 100% | 100% | 100% | 100% |
| Taller Subregional Sobre Ciberseguridad para Sistemas de Control Industrial e Infraestructura Crítica del Sector Eléctrico. (invita OEA, MinDefensa, CNO). | 0% | 0% | 0% | 0% | 0% | 100% | 100% |

## Metodología Implementada

La metodología que se usó en el transcurso del proyecto fue inductiva y descriptiva, ya que a través de una metodología inductiva se analiza solo casos particulares, cuyos resultados son tomados para extraer conclusiones de carácter general, y descriptiva porque no hay manipulación de variables, estas se observan y se describen tal como se presentan en su ambiente natural, es decir, se describe una realidad.

### Actividades a realizar durante el periodo de práctica

- Con base en la Norma ISO 27000 y la metodología de Análisis de ISAGEN, debe coordinar la revisión de la brecha existente entre el modelo de seguridad de la empresa y las normas ISO 27000 versión 2013.

- Realizar un análisis de posibles Casos de uso que de monitoreo para los principales activos y ciberactivos de la empresa, y que permita identificar incidentes de manera oportuna en privacidad y seguridad de la información.

- Apoyar en la ejecución del plan de comunicaciones para el 2017 según las indicaciones y Diseñar los contenidos en los materiales de comunicación para fortalecer los hábitos de seguridad en información de los usuarios, custodios de información y los responsables de la misma en sistemas administrativos e ICS, así como coordinar su revisión y publicación.

- Participar en la implantación de prácticas y controles para fortalecer la postura de seguridad de la empresa de acuerdo con el modelo de seguridad de ISAGEN que se basa en ISO 27000

las normas NERC CIP y el acuerdo CNO 788 y que apoya el cumplimiento de regulatorio relacionado con leyes como SOX, habeas data y transparencia de información pública.

- Participará en el apoyo a la implantación de medidas de seguridad para ICS en lo programado para el semestre II de 2017.

## Resultados

Al inicio de la práctica fue necesario leer toda la documentación que se encontraba en el modelo de seguridad de ISAGEN, ya que a partir de la información que allí se proporciona, se conoce la metodología en cuanto a seguridad e infraestructura que maneja y requiere la empresa.

En el momento de conocer la documentación, al estudiante en práctica se le proporciona permisos de lectura y escritura, para que en el caso que requiera realizar cambios o subir documentos en el modelo de seguridad de la información ubicado en la Intranet (es un sitio web donde se le proporciona información interna a los empleados de ISAGEN), lo pueda hacer.

Para apoyar en la ejecución del plan de comunicaciones para el 2017, se debió diseñar los contenidos en materia de comunicación para fortalecer los hábitos de seguridad en información de los usuarios, custodios y responsables de información en sistemas administrativos e ICS, así como coordinar su revisión y publicación. Por lo tanto, fue necesario la creación de INFORMATIPS, que son tips que enseñan a los trabajadores a cómo proteger y mantener a la empresa segura en caso de posibles ataques ya sea en la información o la infraestructura.

Para realizar un análisis de posibles Casos de uso que de monitoreo para los principales activos y ciberactivos de la empresa, y que permita identificar incidentes de manera oportuna en privacidad y seguridad de la información, se seleccionó los activos más críticos, es decir, los activos que deben tener un mayor cuidado en cuanto a seguridad, y que tienen un nivel de confidencialidad secreta y confidencial, y una disponibilidad crítica y alta.

Se realizó capacitaciones para los trabajadores de ISAGEN, con el fin de explicar el funcionamiento de la herramienta utilizada para tal fin. Esta ha sido creada con el propósito de hacer mucho más fácil el manejo y control de los activos de información de la empresa, por lo que cada responsable de cada activo debe saber en qué consiste su información, como debe manejarla, que responsabilidad tiene sobre ella y si contiene base de datos personales, saber cómo debe ser su tratamiento para que cumpla con las normas estipulados por la Superintendencia de Industria y Comercio (SIC) con la ley 1581.

En ISAGEN es muy importante la seguridad de la información, por lo que se creó estrategias para sensibilizar al trabajador en el cuidado de este activo tan fundamental para la empresa. Por tal motivo, anualmente ISAGEN elabora una encuentra sobre Hábitos de Seguridad para hacer una medición del grado de responsabilidad de los trabajadores en el momento de proteger su información.

ISAGEN contrató la renovación del licenciamiento de Integrity Control para 42 servidores y del SIEM (Security Information and Event Management) de la red SCADA.

ISAGEN contrató la adquisición de un servicio de monitoreo, apoyo en respuesta a incidentes de seguridad de información y, gestión de riesgos y vulnerabilidades en toda la plataforma tanto de tecnologías de información y comunicaciones (TIC) como de sistemas de control industrial (ICS).

Con base en la Norma ISO 27000 y la metodología de Análisis de ISAGEN, se coordinó la revisión de la brecha existente entre el modelo de seguridad de la empresa y las normas ISO 27000 versión 2013.

## Conclusiones

Se conoció la metodología de trabajo que maneja una empresa como ISAGEN para mantener estable su estructura organizacional, además de la importancia en el manejo de la seguridad tanto de la información como la prevención de ciberataques, para conservar y proteger los intereses de la organización.

Se aprendió que no solamente es importante velar por el bienestar e intereses de una empresa, sino también ver la importancia de trabajar en equipo para lograr el cumplimiento de los objetivos que se establecen para llegar a una meta.

ISAGEN por medio de Informatips, les enseña a sus trabajadores a no sólo velar por los intereses y protección de la empresa, sino también por el cuidado, protección y bienestar de ellos mismos. Mi participación permitió la publicación de 21 Informatips e información sobre hábitos de seguridad en la Telerevista y la Revista ENIsagen, construyendo en el cumplimiento del plan de comunicaciones de la empresa. También contribuí en la construcción de un mensaje para Tesorería que mostró la importancia del cuidado de la información en la web.

En la práctica participé de manera activa en las actividades de seguridad de información, logrando tener un contacto directo con las mejoras y adaptaciones del modelo de seguridad de la Información empresarial y los procedimientos asociados, así como las acciones sobre los trabajadores y la tecnología para implementarlo adecuadamente.

Para el análisis de posibles casos de uso que de monitoreo para los principales activos y ciberactivos de la empresa, y que permita identificar incidentes de manera oportuna en privacidad

y seguridad de la información, fue necesario acudir a las personas responsables de dichos activos, para analizar si están manejando la información de manera correcta, y con base a esto determinar si estos activos tienen la protección necesaria que exige ISAGEN para el cuidado de la información.

Para el proceso de capacitación, se mejoró la manera en que se le explica la información a los diferentes responsables, para que puedan tener un mayor entendimiento de las responsabilidades que tienen sobre sus activos.

El área de Gestión de la Información realiza un trabajo continuo para mantener protegidos y seguros los activos de la empresa, por lo que nunca esta demás en mantener el desarrollo de hábitos de seguridad de la información que garanticen su debida protección.

Para el proceso de contratación de un servicio de monitoreo, apoyo en respuesta a incidentes de seguridad de información y, gestión de riesgos y vulnerabilidades en toda la plataforma tanto de tecnologías de información y comunicaciones (TIC) como de sistemas de control industrial (ICS) para ISAGEN, fue necesario la realización de un informe de evaluación y selección de oferta, reuniones con el contratista para determinar y acordar los últimos detalles del contrato, y la elaboración de un checklist con los requisitos que ISAGEN le pidió a la empresa contratada, para asegurar que todo lo requerido si se encontrara en la oferta propuesta.

Todo este proceso fue una gran experiencia, ya que, al participar de este se aprendió como una empresa debe llevar a cabo una contratación para lograr la ejecución de un proyecto. También se evidenció la importancia de estar continuamente evolucionando los mecanismos de seguridad para mantener la estabilidad en materia de protección, permitiendo el avance continuo de ISAGEN.

A raíz de este proyecto, pude participar de la nueva implementación del mecanismo de seguridad en el data center de la empresa, conociendo la infraestructura que ayudara a monitorear y soportar toda la red de ISAGEN, es decir, la red de la sede Medellín y de las 7 centrales (Sogamoso, Miel, Jaguas, Calderas, Termocentro, San Carlos y Amoyá).

Es importante hacer mención de mi participación en las reuniones de "Seguimiento de vulnerabilidades", ya que en estas el equipo de trabajo definía como ha ido manejando las posibles vulnerabilidades que se podían presentar en la empresa. Lo hablado en estas reuniones se debe dejar constancia a través de actas.

Participé en Grupos Primarios, que son reuniones quincenales o mensuales donde se habla de la evolución y avance de los proyectos que se llevan a cabo en cada equipo de trabajo, y junto con esto se estipula una fecha límite de entrega para cada proyecto. A esto también se le suma el TBI, que es una reunión que tiene cada encargado de cierto proceso para presentar el avance y finalización de cierta actividad, en el caso que no cumpla con la actividad estipulada para dicha fecha, implica atraso en el cronograma de actividades que se maneja, perjudicando el desempeño y cumplimiento que debe tener la empresa. Todos estos procesos enseñan a mantener la disciplina y trabajo constante para lograr los objetivos establecidos.

De igual manera aprendí en cada reunión que fui convocada por mi tutor de práctica, la manera como se lleva a cabo asuntos y actividades importantes en la empresa, y de igual forma la manera como se debe dar respuesta a cada una de ellas para determinar cuál es la solución correcta a cada proceso que se debe llevar a cabo.

He aportado en la realización de un informe donde se menciona como se encuentra la matriz de riesgos de los activos de información de la empresa, y que se debe hacer para que el riesgo del activo sea bajo y no crítico.

Participé en la construcción de una exposición sobre el manejo de información confidencial para la Secretaria General de ISAGEN, lo cual fue muy importante porque contribuí al desarrollo de las buenas prácticas del manejo de la información y seguridad cibernética.

Al mismo tiempo contribuí en la actualización de los documentos del Modelo de Seguridad de la empresa, lo cual es importante para mantener actualizada la continuidad del negocio.

Asistí al evento Fortinet Cybersecurity Summit 2017, que fue un espacio de diálogo entre expertos y profesionales, donde se habló por qué la Ciberseguridad es uno de los principales habilitadores de negocio en una empresa.

Forme parte de la logística del Taller Subregional Sobre Ciberseguridad para Sistemas de Control Industrial e Infraestructura Crítica del Sector Eléctrico. (invita OEA, MinDefensa, CNO), lo cual fue una experiencia muy enriquecedora para mi vida profesional.

En la coordinación de la revisión de la brecha existente entre el modelo de seguridad de la empresa y las normas ISO 27000 versión 2013, se realizó un checklist con el propósito de analizar el nivel de cumplimiento de ISAGEN en esta norma.

También es importante destacar mi participación en el cierre del TBI de fin de año, en donde se logró finalizar objetivos importantes para la empresa como la documentación transversal crítica para una central.

Finalmente, como recomendación para el desarrollo profesional del estudiante de la Universidad Santo Tomás y con base a la experiencia vivida en ISAGEN, es fundamental que se les dé más profundización a materias como ciberseguridad y administración, y también un enfoque en la redacción de informes, ya que son vitales en el momento de presentar resultados en una empresa. Con esto el profesional que se enfrente a este tipo de situación tendrá todas las capacidades necesarias para enfrentarlas.

## Referencias

Berciano, J. (s.f). *redseguridad.com*. Recuperado el 05 de Noviembre de 2017, de http://www.redseguridad.com/especialidades-tic/proteccion-de-datos/la-importancia-y-la-necesidad-de-proteger-la-informacion-sensible

Díaz Hernández , M. (25 de Agosto de 2015). *Hipertextual*. Recuperado el 06 de Noviembre de 2017, de https://hipertextual.com/2015/08/que-es-el-spear-phishing

ISAGEN. (s.f.). *ISAGEN energía productiva*. Recuperado el 06 de Noviembre de 2017, de https://www.isagen.com.co/SitioWeb/es/nosotros/quienes-somos